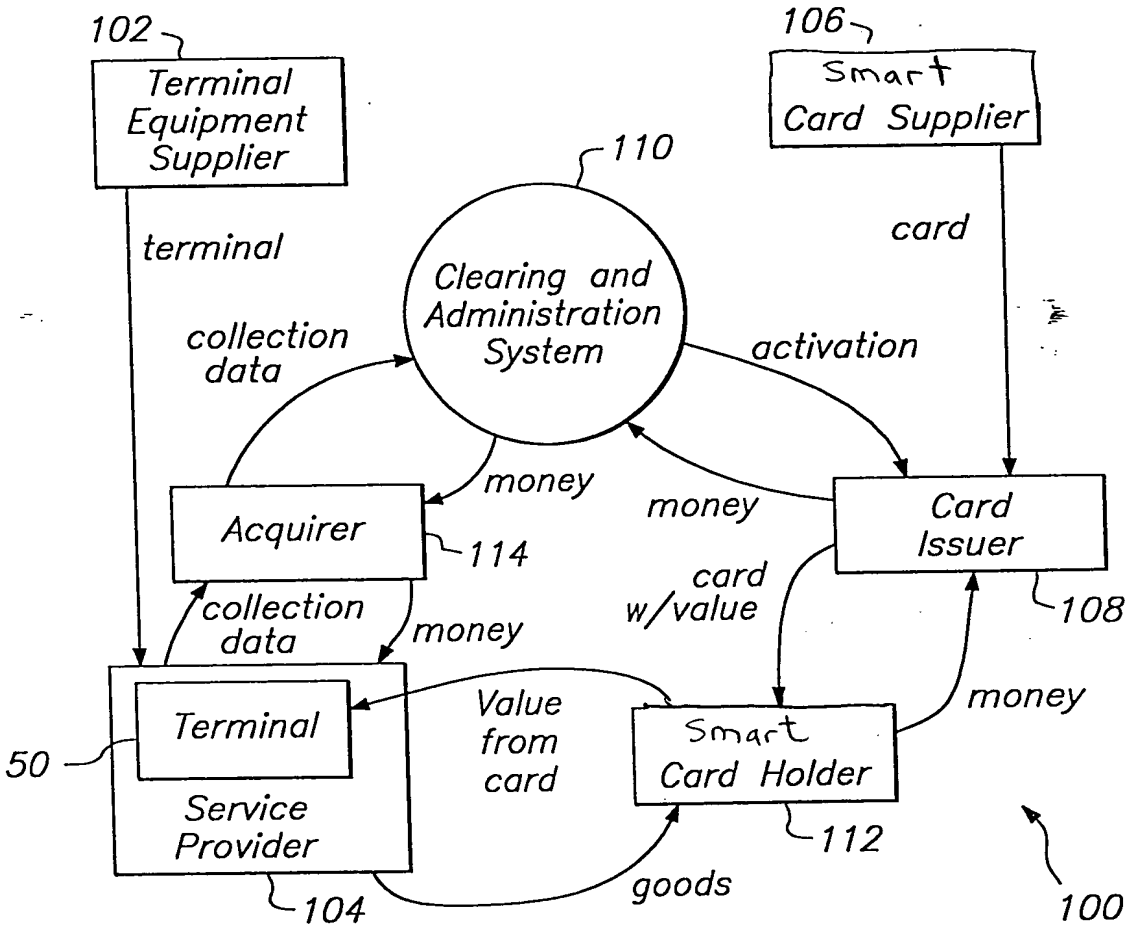


FIG. 1 PRIOR ART

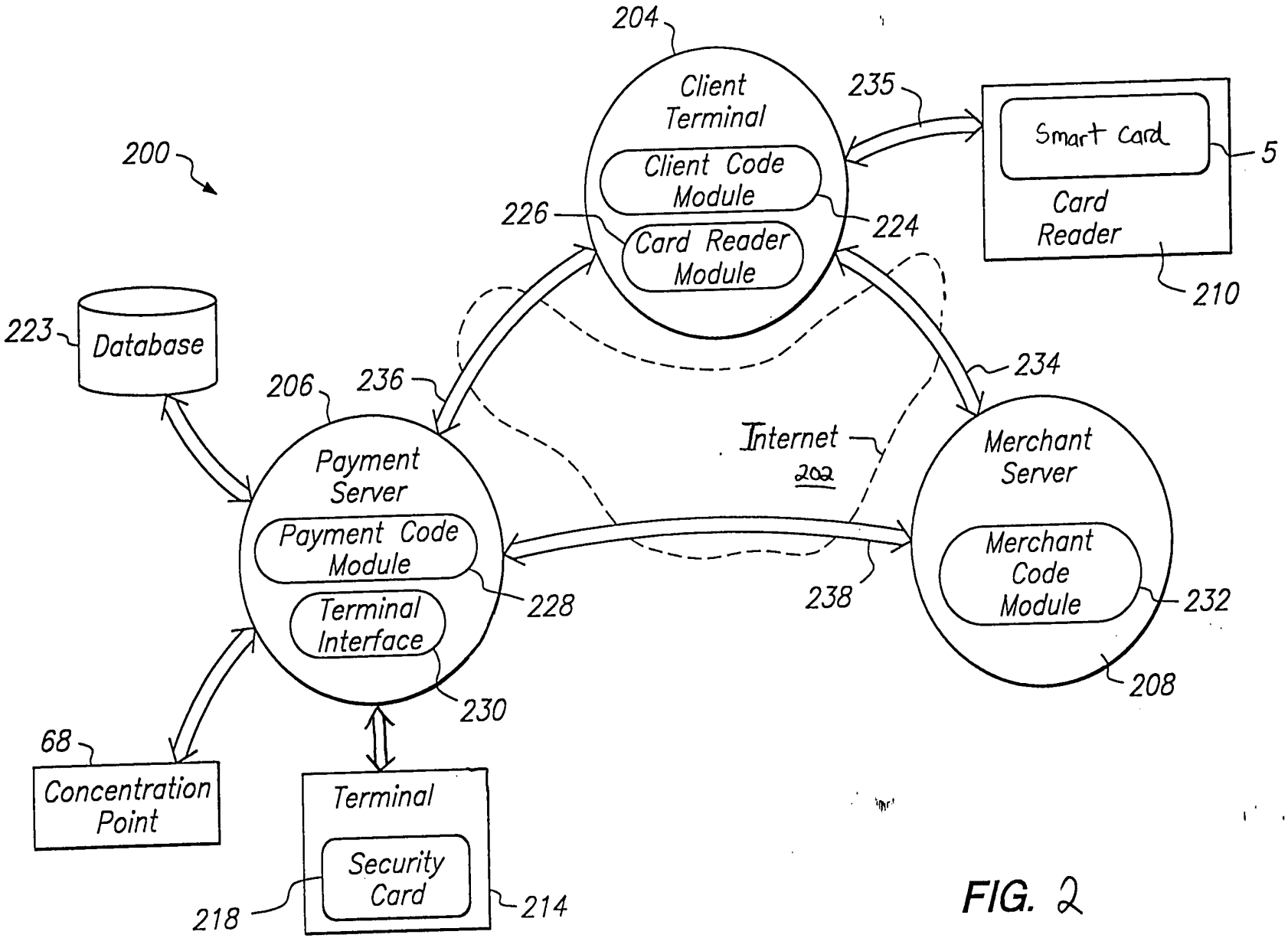


FIG. 2

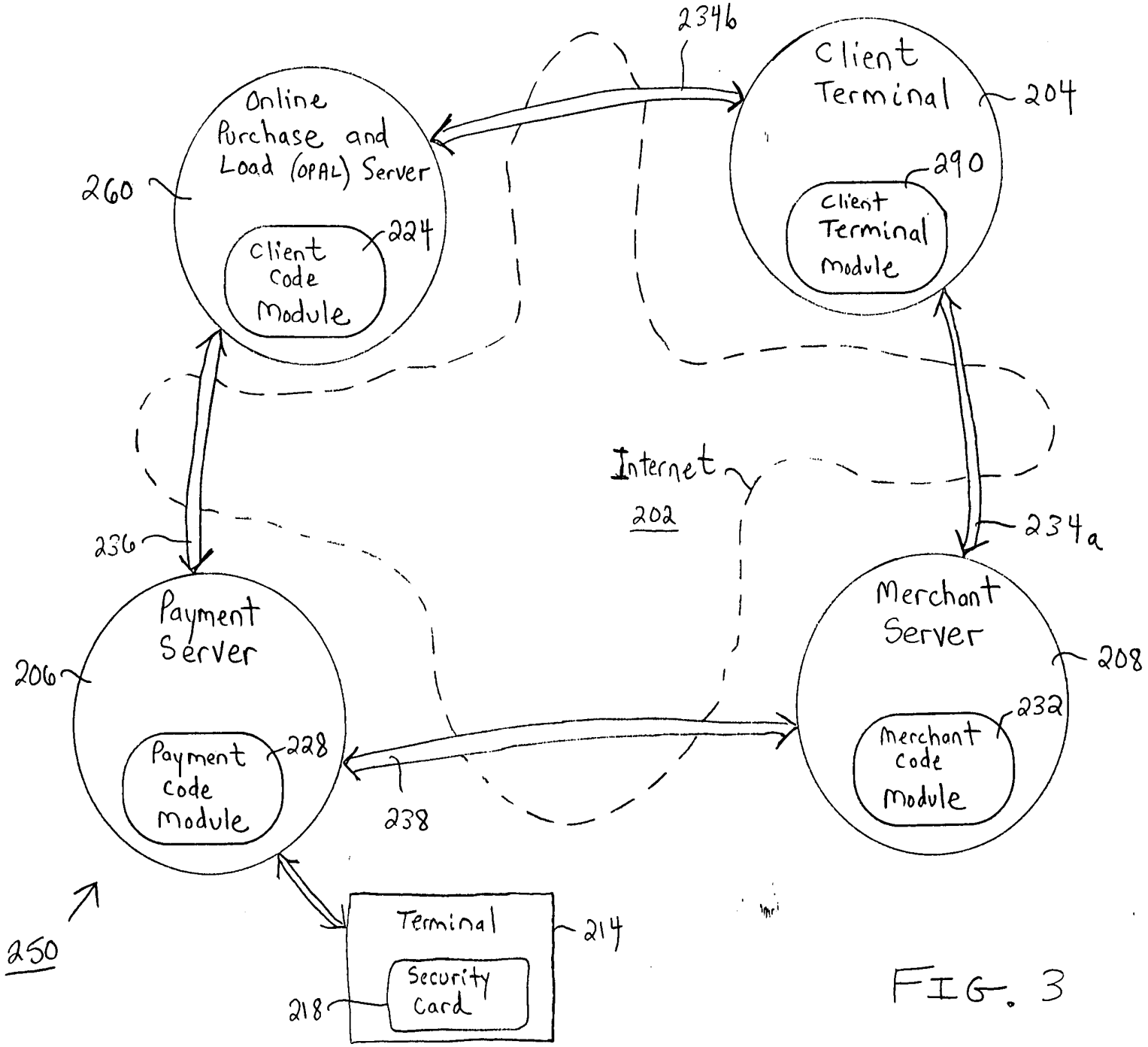
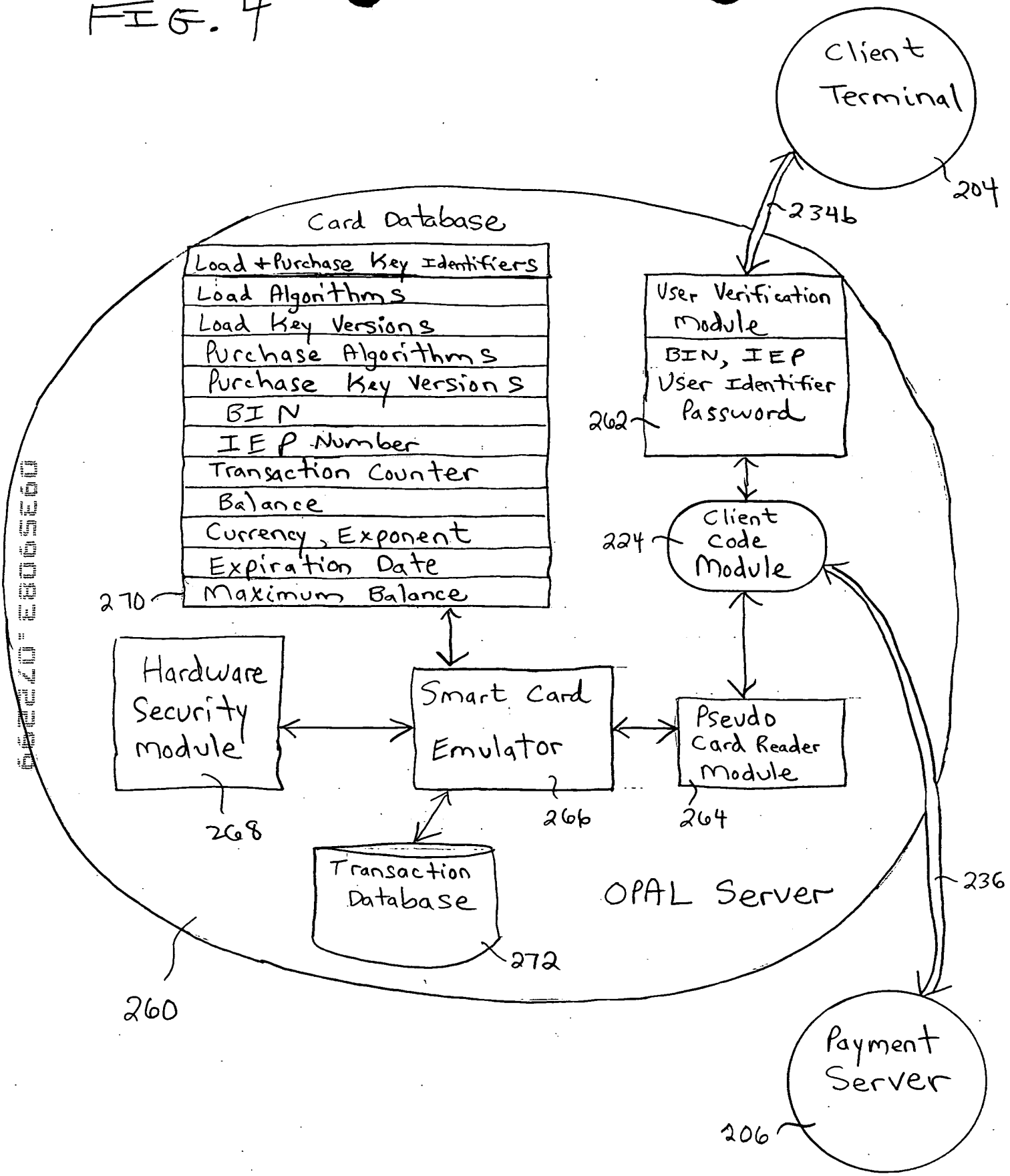

2346
Client Terminal
204
Online Purchase and Load (OPAL) Server
260
290
Client Terminal Module
224
Client Code Module
Internet
202
234a
236
Payment Server
206
Merchant Server
208
232
Merchant code module
228
Payment code module
238
250
Terminal
214
Security Card
218

FIG. 3

FIG. 4


Client Terminal
204
234b
Card Database
Load + Purchase Key Identifiers
Load Algorithms
Load Key Versions
Purchase Algorithms
Purchase Key Versions
BIN
IEP Number
Transaction Counter
Balance
Currency, Exponent
Expiration Date
Maximum Balance
270
User Verification Module
BIN, IEP
User Identifier
Password
262
Client Code Module
224
Hardware Security module
268
Smart Card Emulator
266
Pseudo Card Reader Module
264
Transaction Database
272
OPAL Server
260
236
Payment Server
206

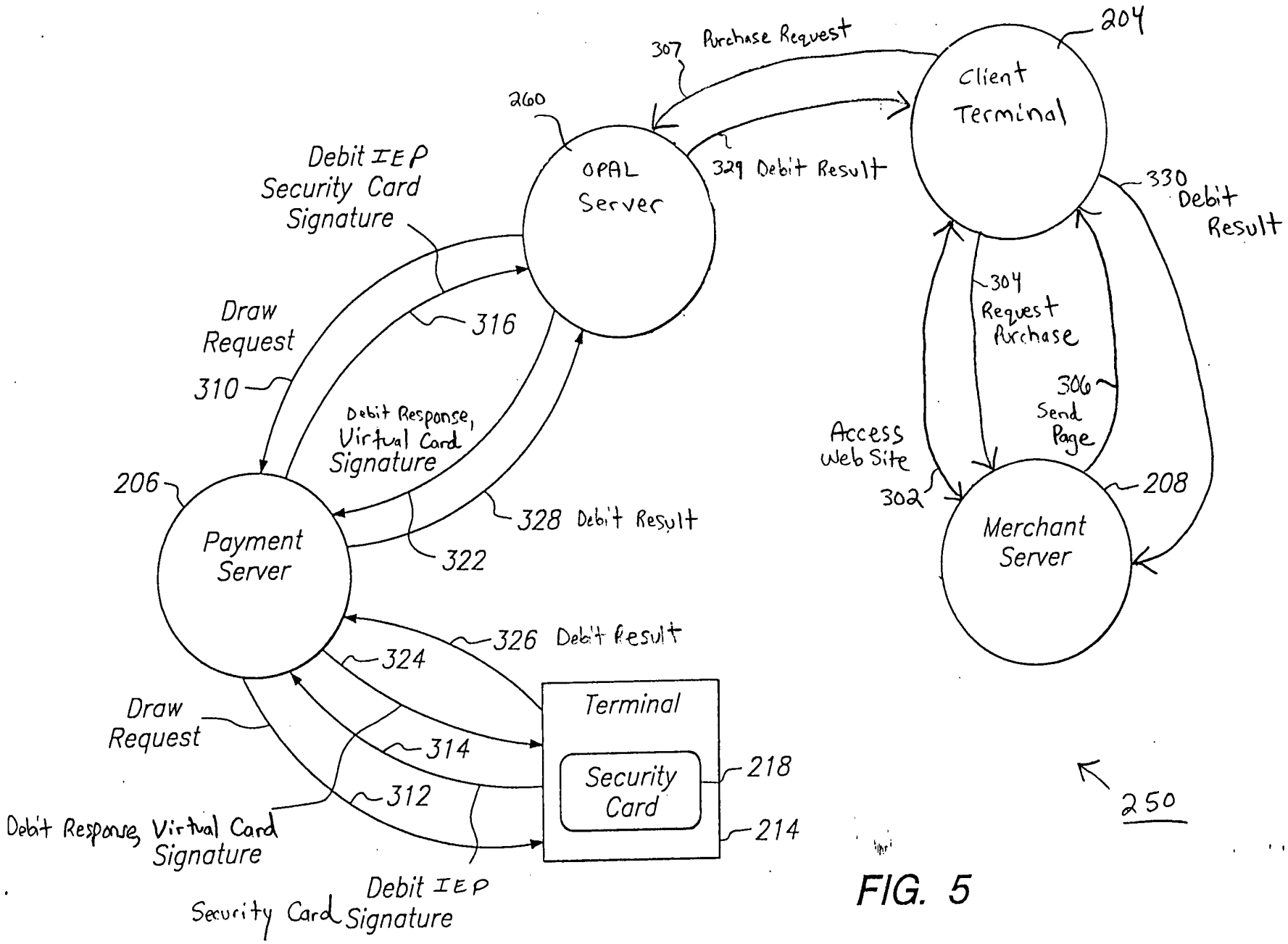

307 Purchase Request
204
Client Terminal
260
OPAL Server
329 Debit Result
330 Debit Result
Debit IEP Security Card Signature
Draw Request
310
316
304 Request Purchase
306 Send Page
Access Web Site
302
208
Merchant Server
Debit Response, Virtual Card Signature
206
Payment Server
328 Debit Result
322
326 Debit Result
324
Terminal
Draw Request
314
Security Card
218
312
214
Debit Response, Virtual Card Signature
Debit IEP Security Card Signature
250

FIG. 5

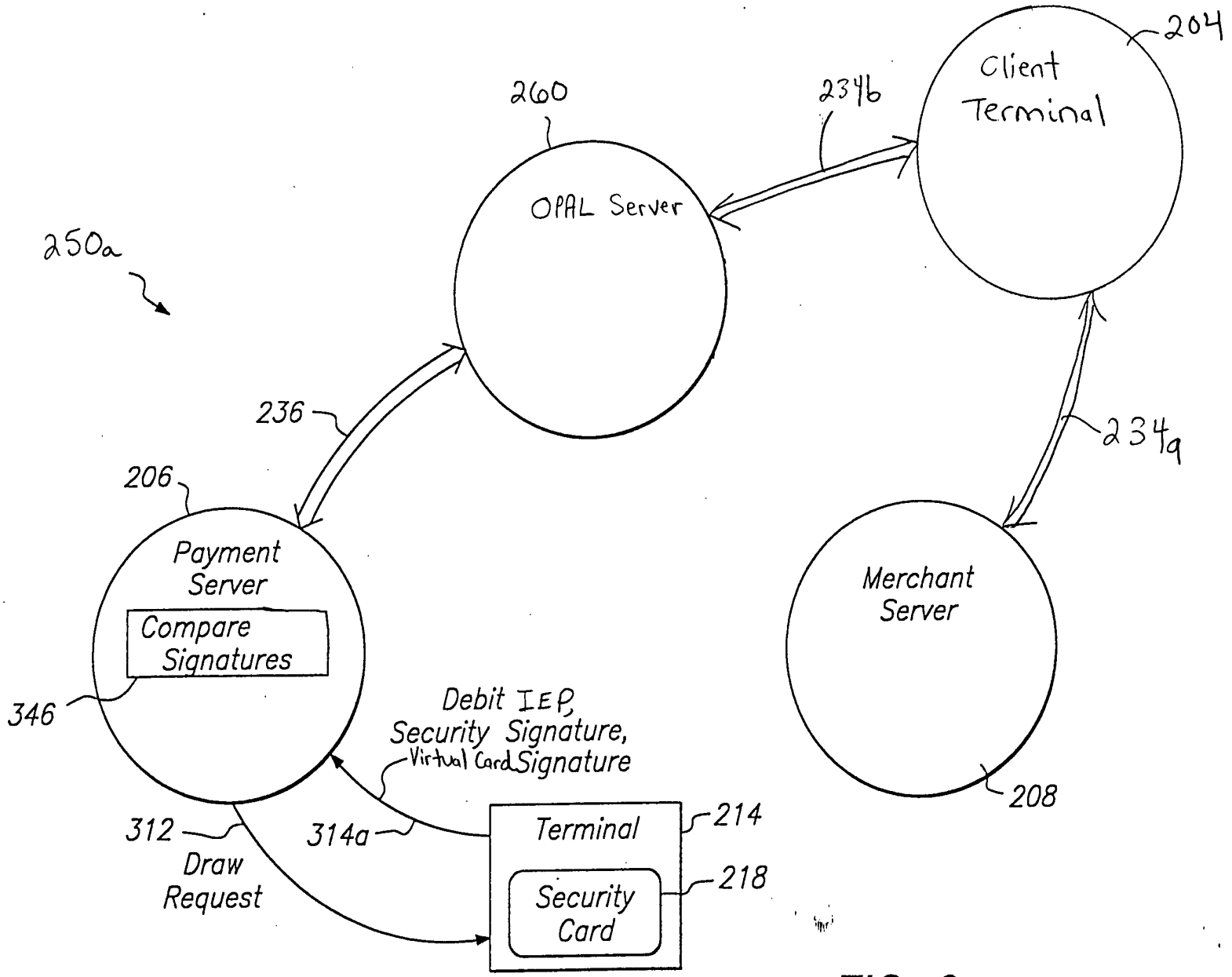


FIG. 6

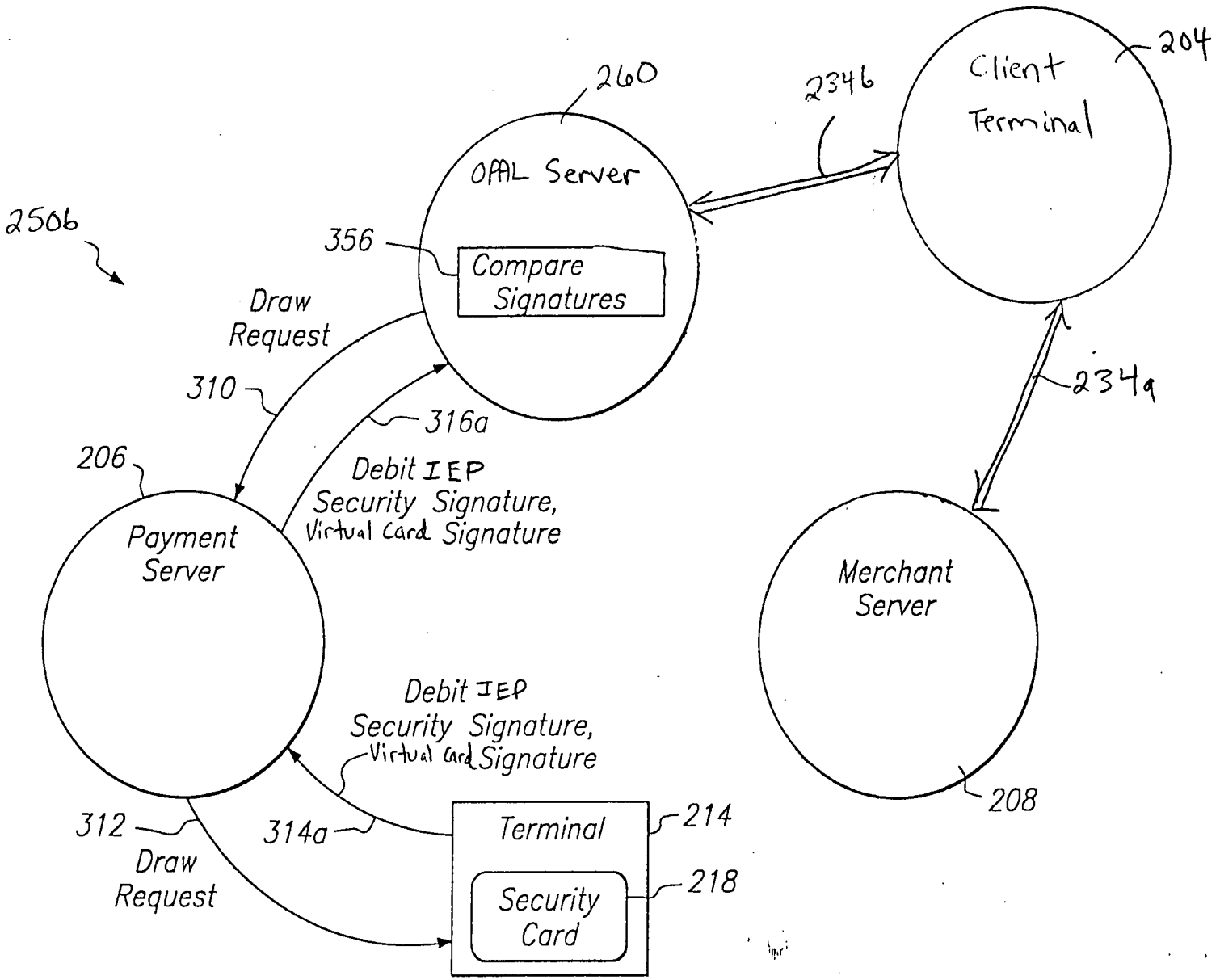

2506
260
OPAL Server
356
Compare Signatures
2346
Client Terminal
204
Draw Request
310
316a
Debit IEP Security Signature, Virtual Card Signature
206
Payment Server
234a
Merchant Server
208
Debit IEP Security Signature, Virtual Card Signature
312
Draw Request
314a
Terminal
214
Security Card
218

FIG. 7

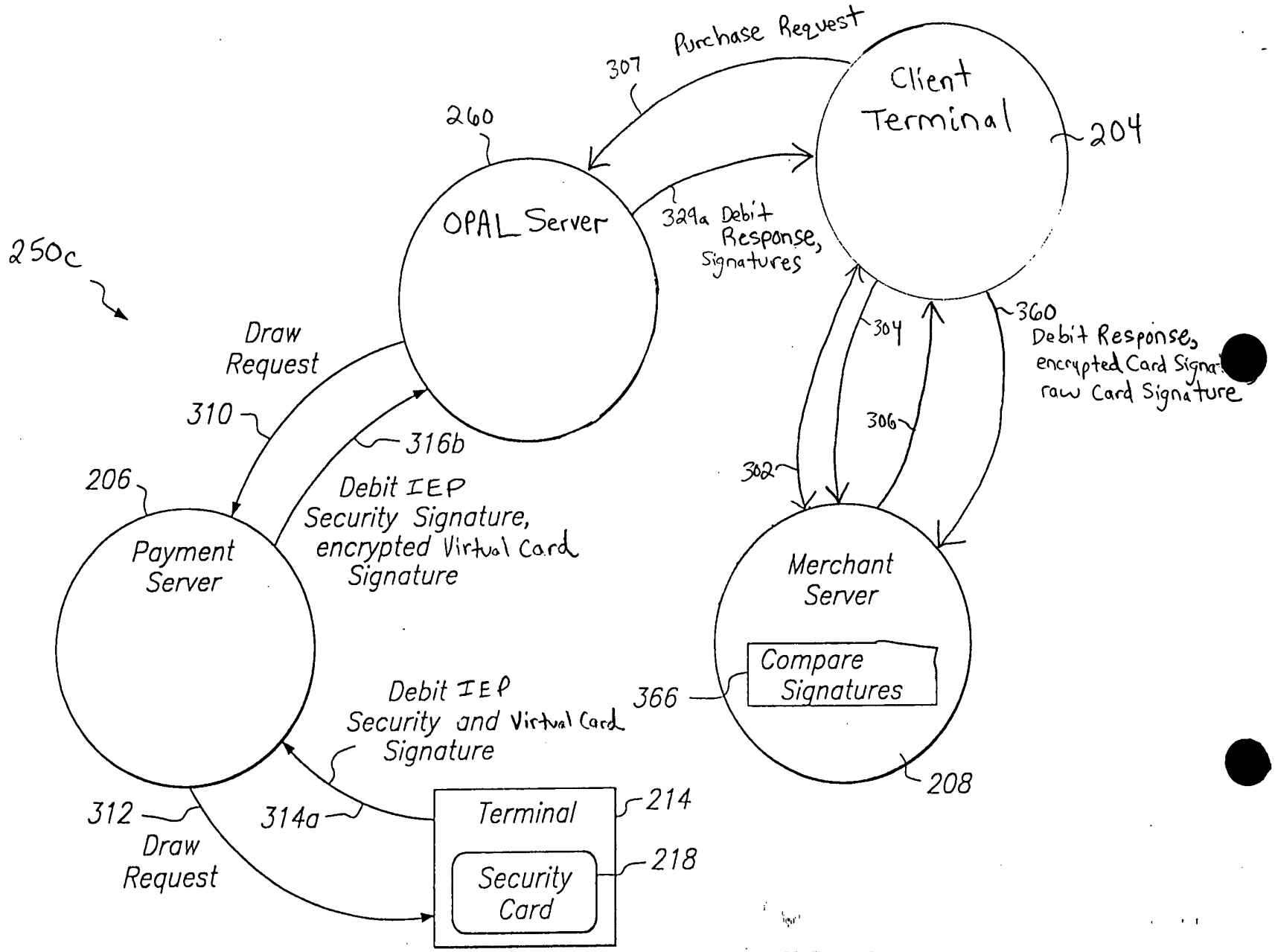

250c
Purchase Request
307
260
OPAL Server
Client Terminal
204
329a Debit Response, Signatures
Draw Request
310
316b
206
Payment Server
Debit IEP Security Signature, encrypted Virtual Card Signature
304
306
302
360
Debit Response, encrypted Card Signature, raw Card Signature
Merchant Server
Compare Signatures
366
208
Debit IEP Security and Virtual Card Signature
312
Draw Request
314a
Terminal
214
Security Card
218

FIG. 8

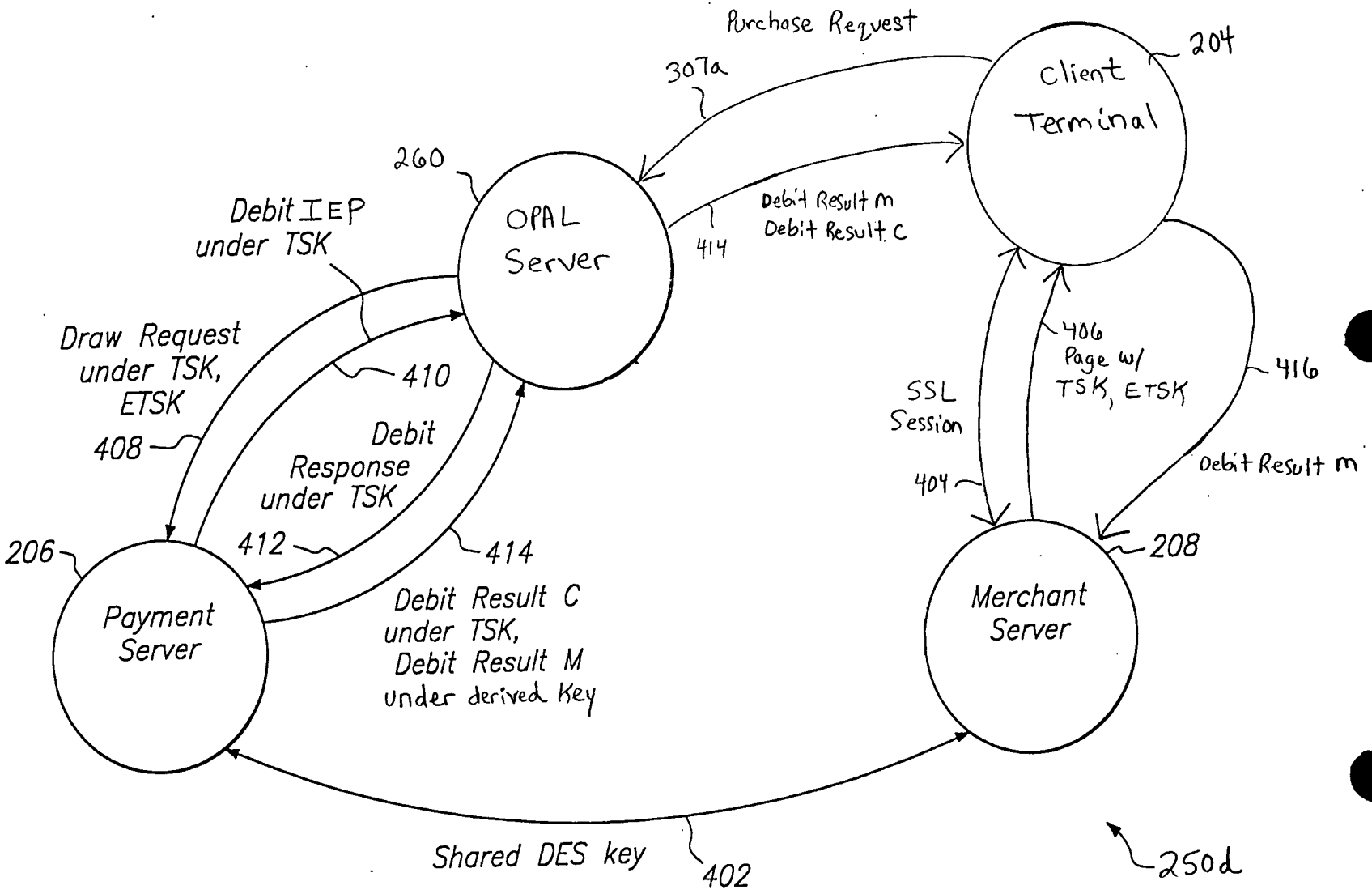

Purchase Request
307a
204
Client Terminal
260
OPAL Server
Debit IEP under TSK
Debit Result M
Debit Result C
414
Draw Request under TSK, ETSK
408
410
Debit Response under TSK
412
414
206
Payment Server
Debit Result C under TSK, Debit Result M under derived key
SSL Session
404
406 Page w/ TSK, ETSK
416
Debit Result M
208
Merchant Server
Shared DES key
402
250d

FIG. 9

FIG. 10

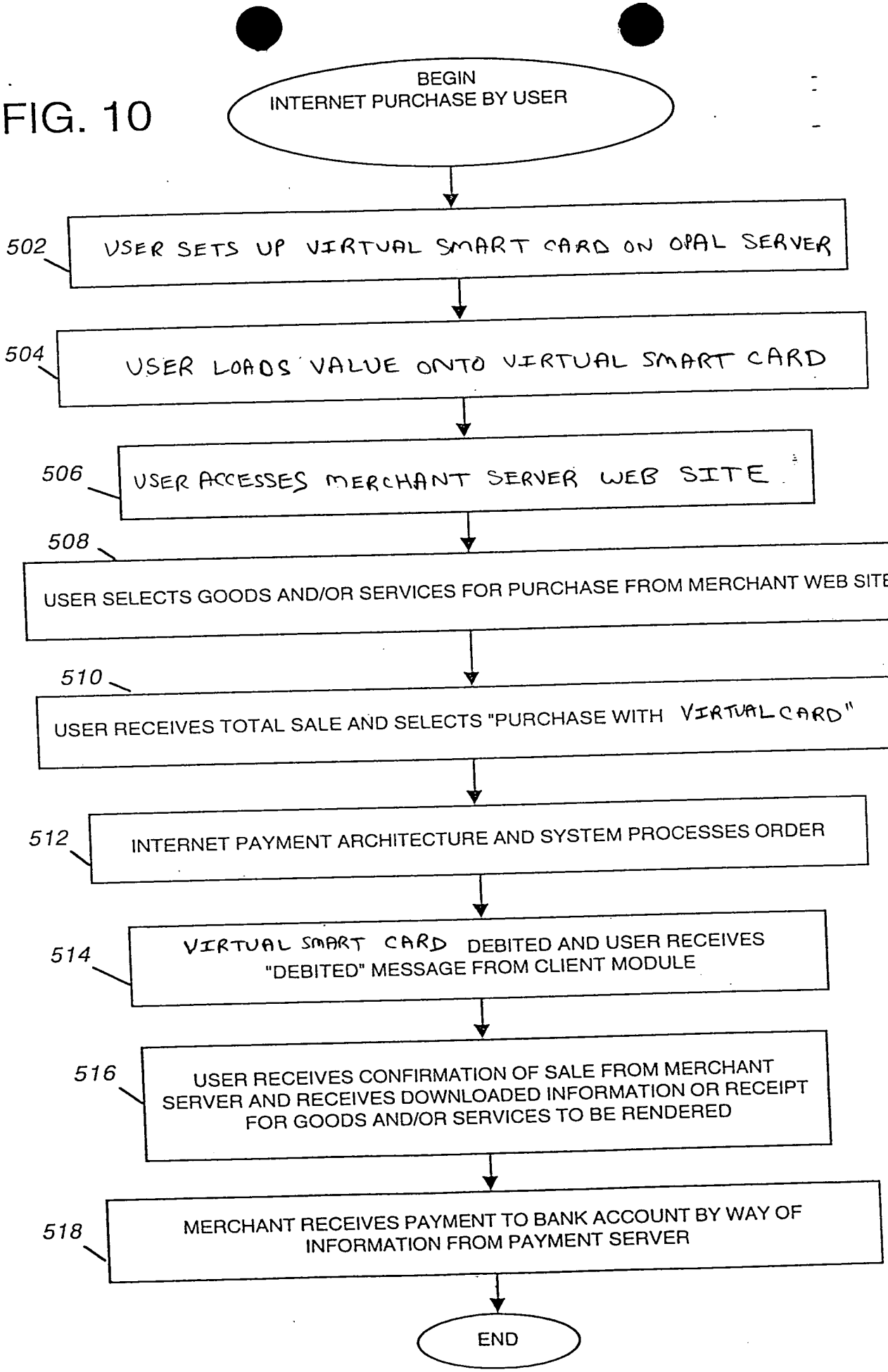

BEGIN
INTERNET PURCHASE BY USER
502
USER SETS UP VIRTUAL SMART CARD ON OPAL SERVER
504
USER LOADS VALUE ONTO VIRTUAL SMART CARD
506
USER ACCESSES MERCHANT SERVER WEB SITE
508
USER SELECTS GOODS AND/OR SERVICES FOR PURCHASE FROM MERCHANT WEB SITE
510
USER RECEIVES TOTAL SALE AND SELECTS "PURCHASE WITH VIRTUAL CARD"
512
INTERNET PAYMENT ARCHITECTURE AND SYSTEM PROCESSES ORDER
514
VIRTUAL SMART CARD DEBITED AND USER RECEIVES "DEBITED" MESSAGE FROM CLIENT MODULE
516
USER RECEIVES CONFIRMATION OF SALE FROM MERCHANT SERVER AND RECEIVES DOWNLOADED INFORMATION OR RECEIPT FOR GOODS AND/OR SERVICES TO BE RENDERED
518
MERCHANT RECEIVES PAYMENT TO BANK ACCOUNT BY WAY OF INFORMATION FROM PAYMENT SERVER
END

FIG. 11A

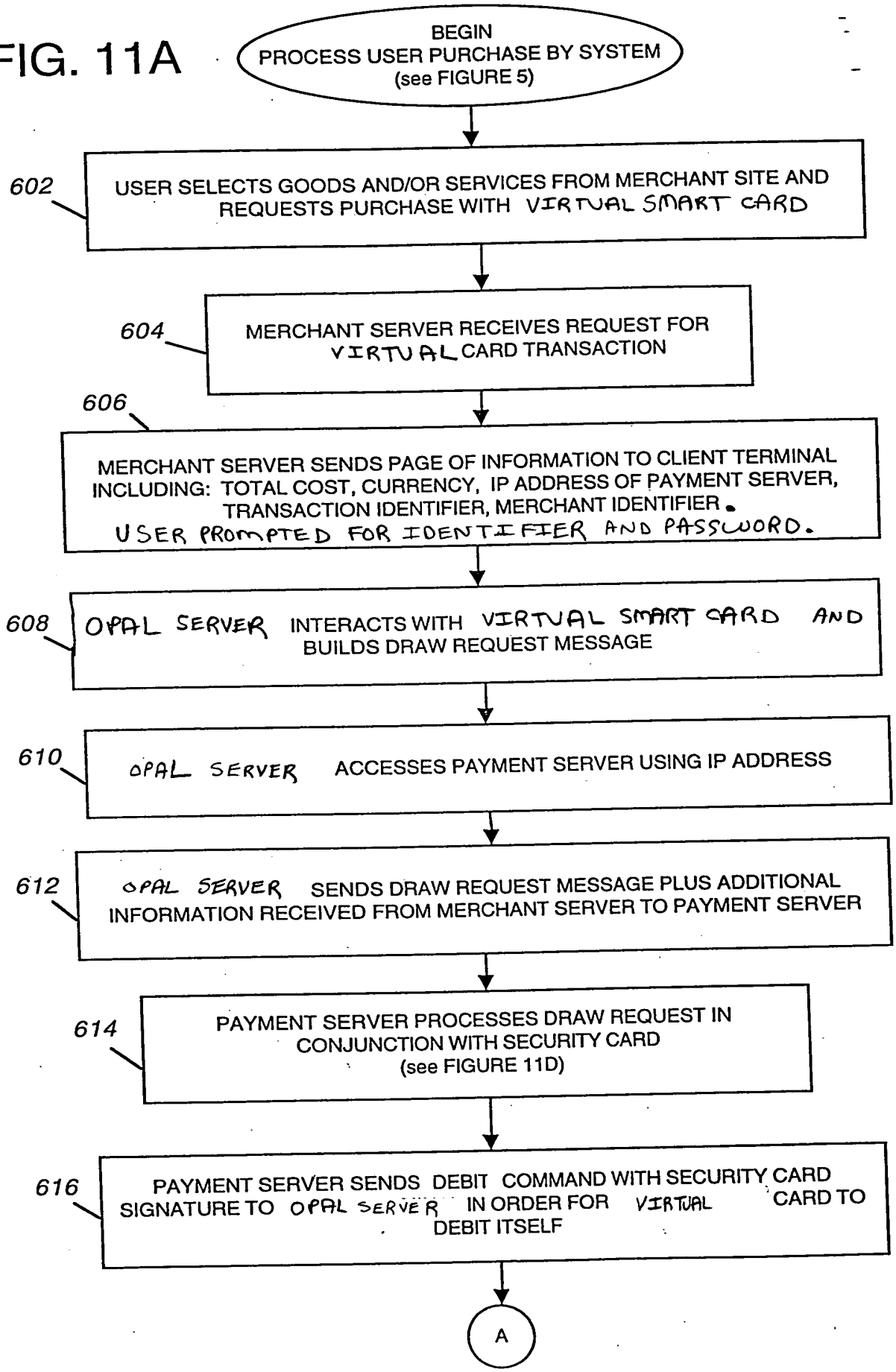
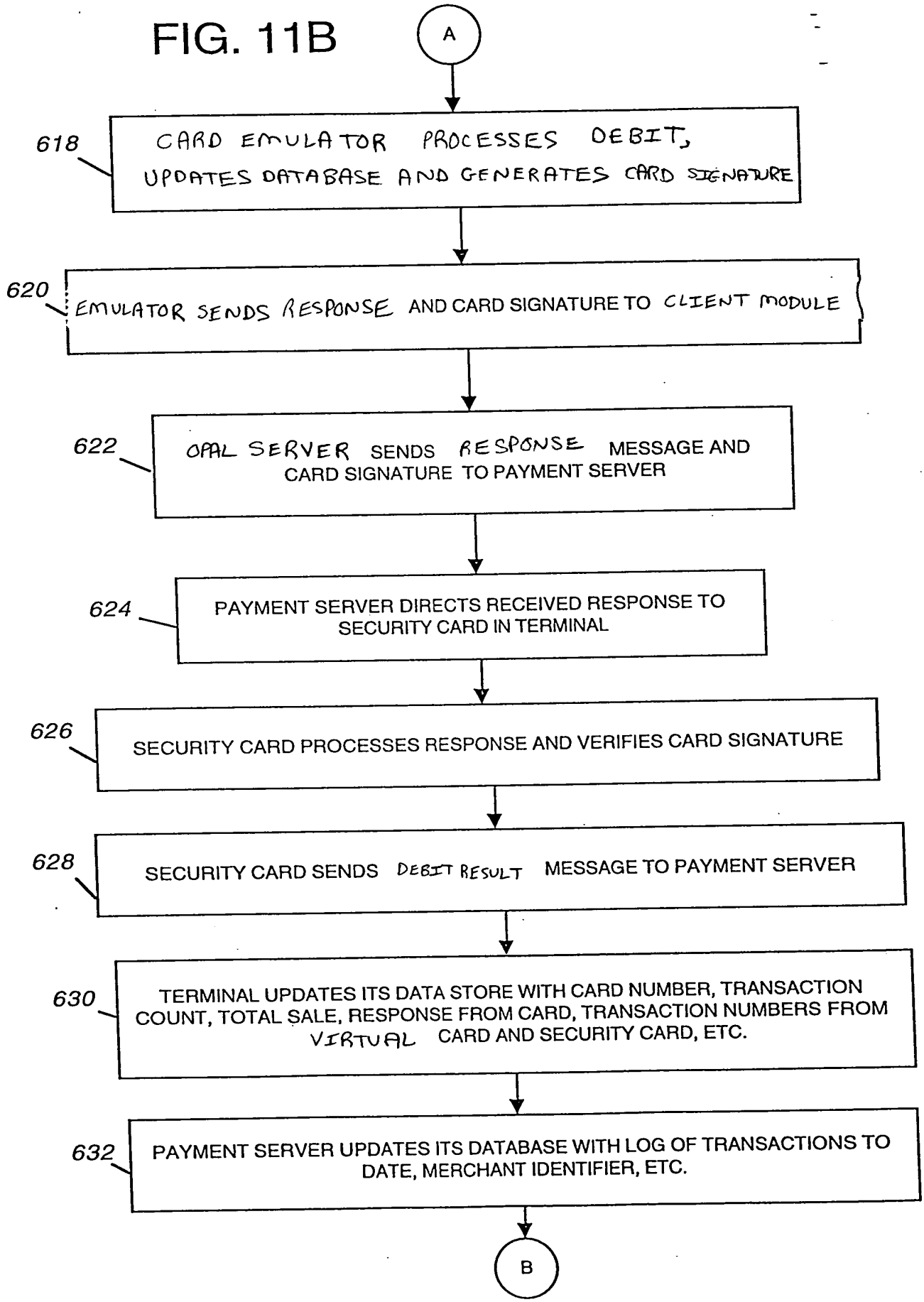

BEGIN
PROCESS USER PURCHASE BY SYSTEM
(see FIGURE 5)
602
USER SELECTS GOODS AND/OR SERVICES FROM MERCHANT SITE AND REQUESTS PURCHASE WITH VIRTUAL SMART CARD
604
MERCHANT SERVER RECEIVES REQUEST FOR VIRTUAL CARD TRANSACTION
606
MERCHANT SERVER SENDS PAGE OF INFORMATION TO CLIENT TERMINAL INCLUDING: TOTAL COST, CURRENCY, IP ADDRESS OF PAYMENT SERVER, TRANSACTION IDENTIFIER, MERCHANT IDENTIFIER.
USER PROMPTED FOR IDENTIFIER AND PASSWORD.
608
OPAL SERVER INTERACTS WITH VIRTUAL SMART CARD AND BUILDS DRAW REQUEST MESSAGE
610
OPAL SERVER ACCESSES PAYMENT SERVER USING IP ADDRESS
612
OPAL SERVER SENDS DRAW REQUEST MESSAGE PLUS ADDITIONAL INFORMATION RECEIVED FROM MERCHANT SERVER TO PAYMENT SERVER
614
PAYMENT SERVER PROCESSES DRAW REQUEST IN CONJUNCTION WITH SECURITY CARD
(see FIGURE 11D)
616
PAYMENT SERVER SENDS DEBIT COMMAND WITH SECURITY CARD SIGNATURE TO OPAL SERVER IN ORDER FOR VIRTUAL CARD TO DEBIT ITSELF
A

FIG. 11B


A
618
CARD EMULATOR PROCESSES DEBIT, UPDATES DATABASE AND GENERATES CARD SIGNATURE
620
EMULATOR SENDS RESPONSE AND CARD SIGNATURE TO CLIENT MODULE
622
OPAL SERVER SENDS RESPONSE MESSAGE AND CARD SIGNATURE TO PAYMENT SERVER
624
PAYMENT SERVER DIRECTS RECEIVED RESPONSE TO SECURITY CARD IN TERMINAL
626
SECURITY CARD PROCESSES RESPONSE AND VERIFIES CARD SIGNATURE
628
SECURITY CARD SENDS DEBIT RESULT MESSAGE TO PAYMENT SERVER
630
TERMINAL UPDATES ITS DATA STORE WITH CARD NUMBER, TRANSACTION COUNT, TOTAL SALE, RESPONSE FROM CARD, TRANSACTION NUMBERS FROM VIRTUAL CARD AND SECURITY CARD, ETC.
632
PAYMENT SERVER UPDATES ITS DATABASE WITH LOG OF TRANSACTIONS TO DATE, MERCHANT IDENTIFIER, ETC.
B

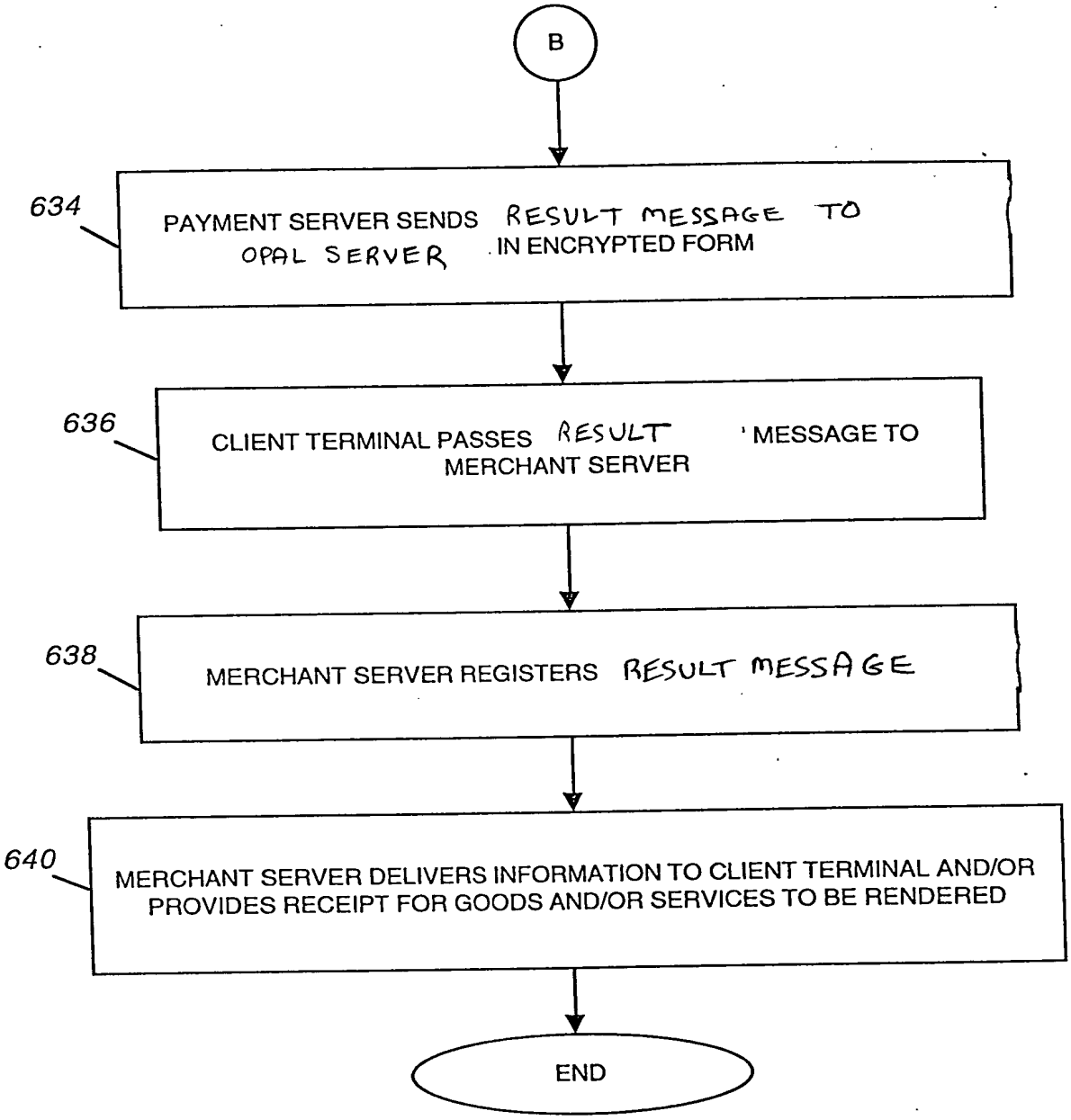
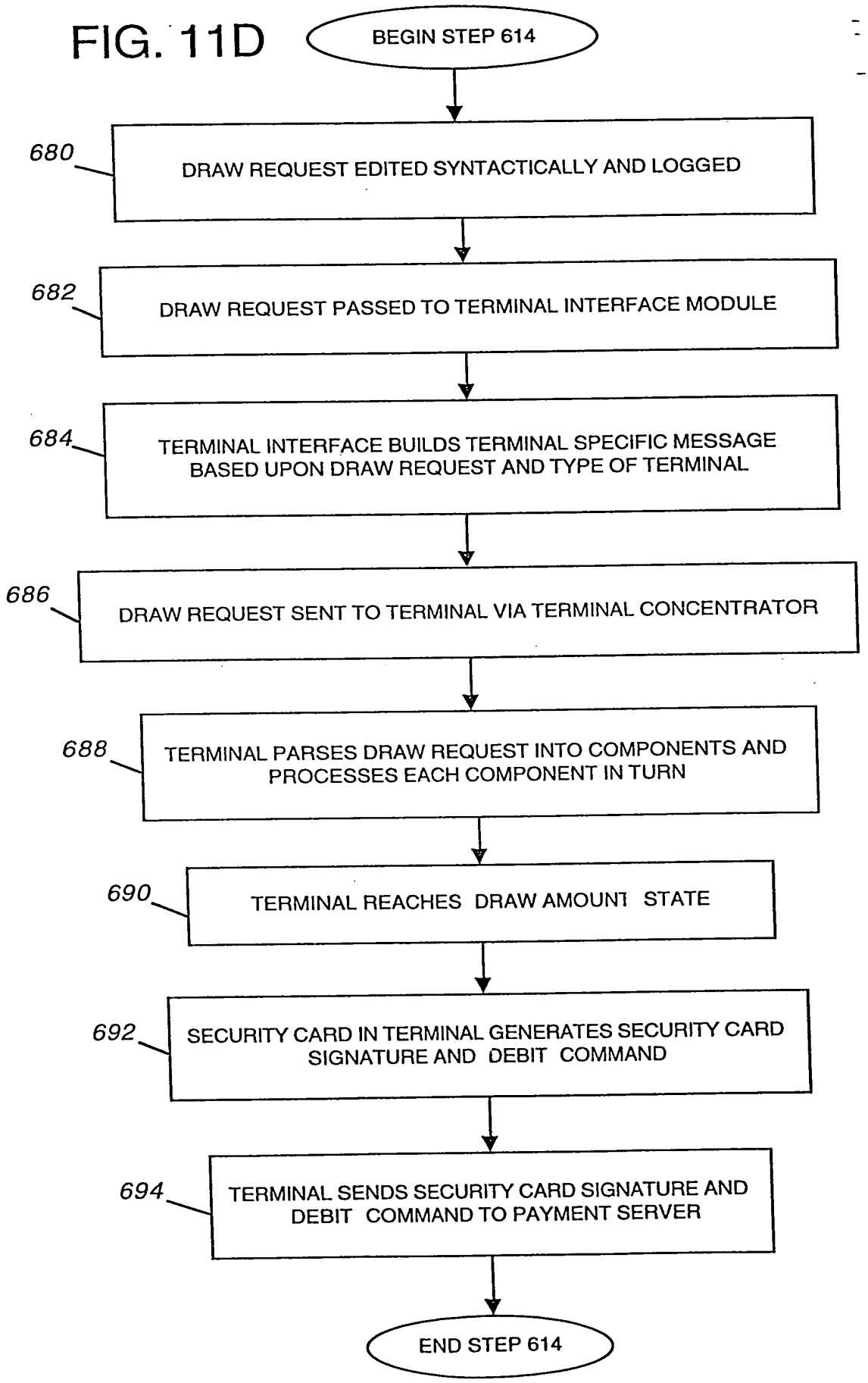

B
634
PAYMENT SERVER SENDS RESULT MESSAGE TO OPAL SERVER IN ENCRYPTED FORM
636
CLIENT TERMINAL PASSES RESULT MESSAGE TO MERCHANT SERVER
638
MERCHANT SERVER REGISTERS RESULT MESSAGE
640
MERCHANT SERVER DELIVERS INFORMATION TO CLIENT TERMINAL AND/OR PROVIDES RECEIPT FOR GOODS AND/OR SERVICES TO BE RENDERED
END

FIG. 11C

FIG. 11D


BEGIN STEP 614
680
DRAW REQUEST EDITED SYNTACTICALLY AND LOGGED
682
DRAW REQUEST PASSED TO TERMINAL INTERFACE MODULE
684
TERMINAL INTERFACE BUILDS TERMINAL SPECIFIC MESSAGE BASED UPON DRAW REQUEST AND TYPE OF TERMINAL
686
DRAW REQUEST SENT TO TERMINAL VIA TERMINAL CONCENTRATOR
688
TERMINAL PARSES DRAW REQUEST INTO COMPONENTS AND PROCESSES EACH COMPONENT IN TURN
690
TERMINAL REACHES DRAW AMOUNT STATE
692
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE AND DEBIT COMMAND
694
TERMINAL SENDS SECURITY CARD SIGNATURE AND DEBIT COMMAND TO PAYMENT SERVER
END STEP 614

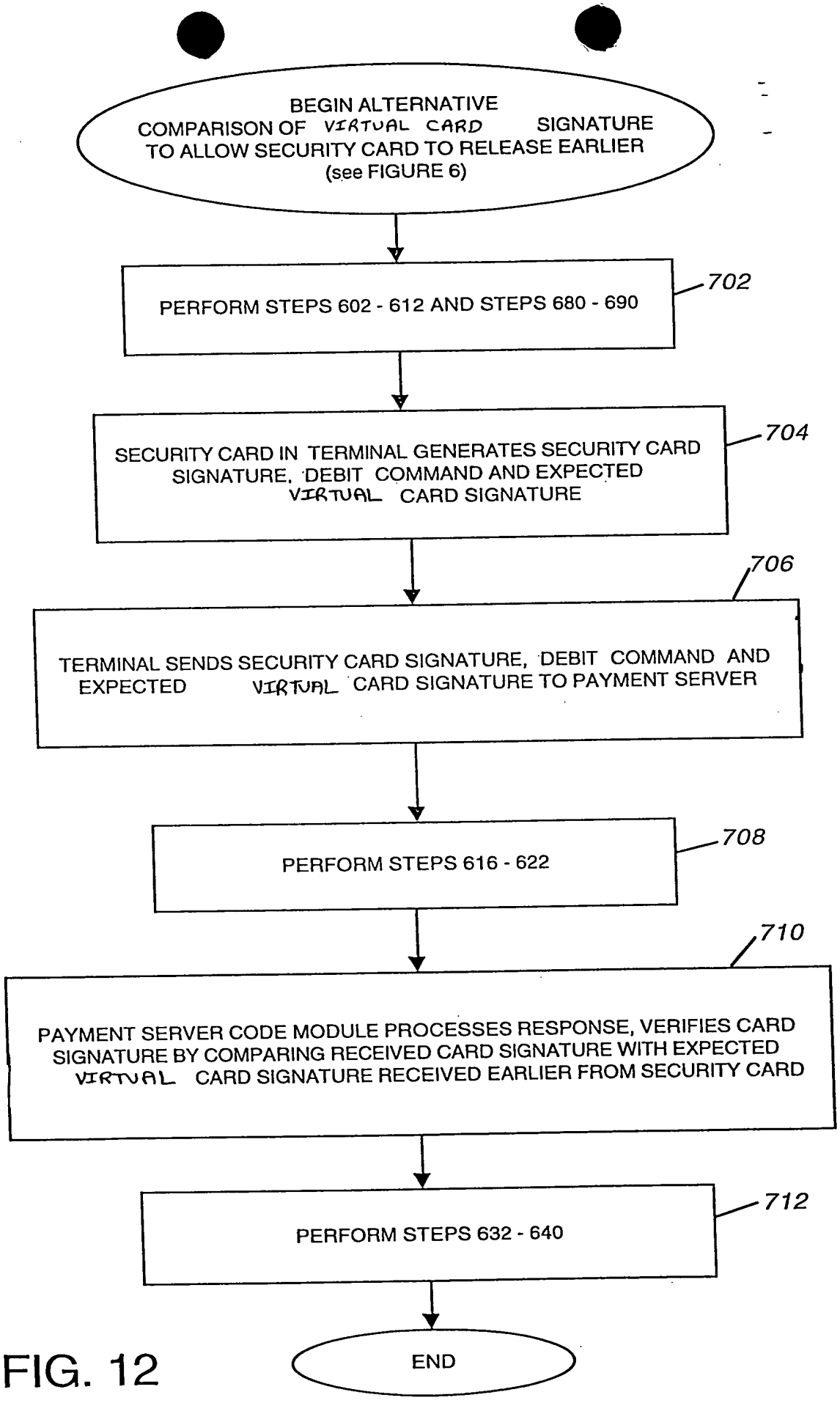

BEGIN ALTERNATIVE COMPARISON OF VIRTUAL CARD SIGNATURE TO ALLOW SECURITY CARD TO RELEASE EARLIER (see FIGURE 6)
PERFORM STEPS 602 - 612 AND STEPS 680 - 690
702
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE
704
706
TERMINAL SENDS SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE TO PAYMENT SERVER
PERFORM STEPS 616 - 622
708
710
PAYMENT SERVER CODE MODULE PROCESSES RESPONSE, VERIFIES CARD SIGNATURE BY COMPARING RECEIVED CARD SIGNATURE WITH EXPECTED VIRTUAL CARD SIGNATURE RECEIVED EARLIER FROM SECURITY CARD
PERFORM STEPS 632 - 640
712
END

FIG. 12

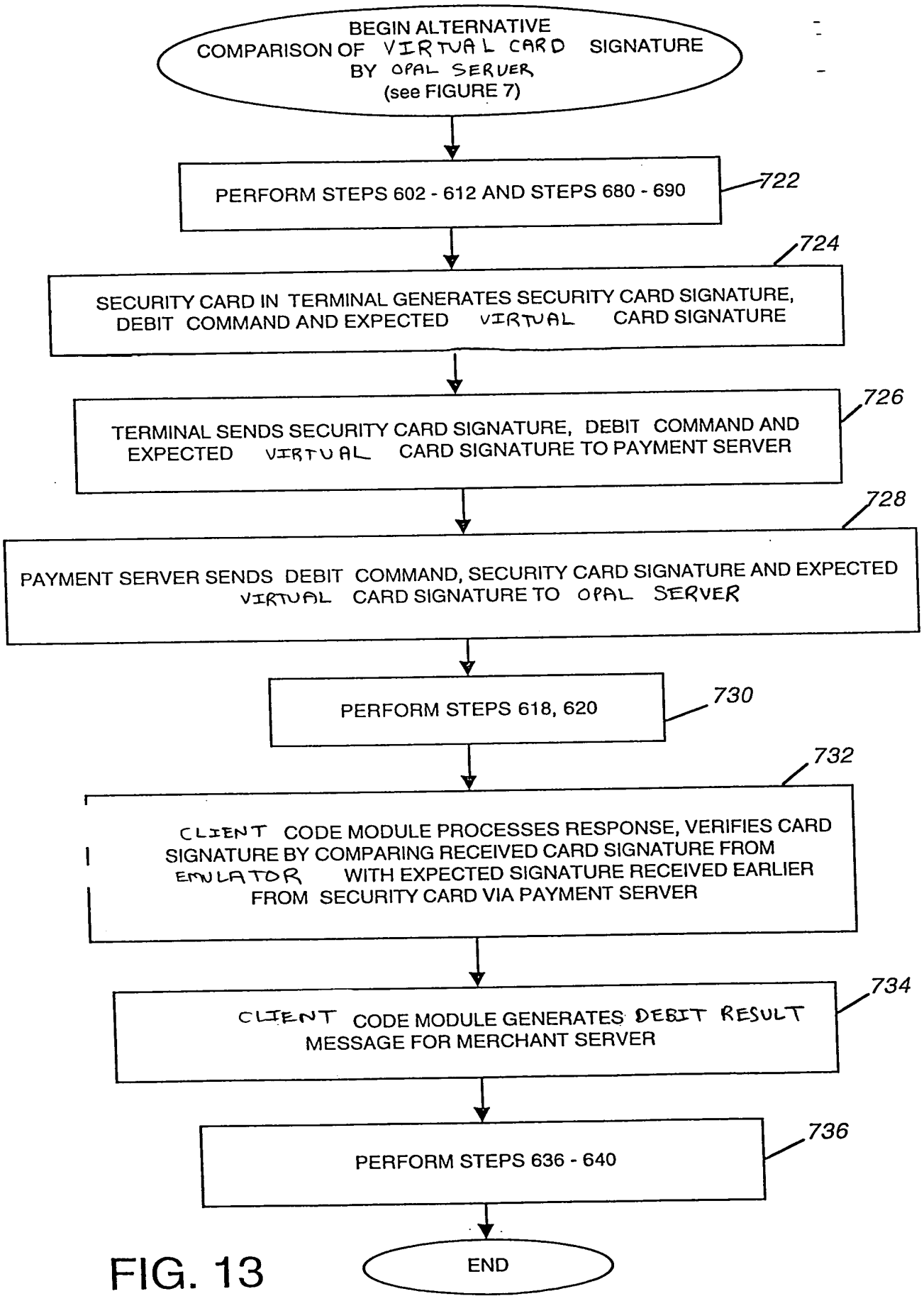

BEGIN ALTERNATIVE COMPARISON OF VIRTUAL CARD SIGNATURE BY OPAL SERVER (see FIGURE 7)
PERFORM STEPS 602 - 612 AND STEPS 680 - 690
722
724
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE
726
TERMINAL SENDS SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE TO PAYMENT SERVER
728
PAYMENT SERVER SENDS DEBIT COMMAND, SECURITY CARD SIGNATURE AND EXPECTED VIRTUAL CARD SIGNATURE TO OPAL SERVER
PERFORM STEPS 618, 620
730
732
CLIENT CODE MODULE PROCESSES RESPONSE, VERIFIES CARD SIGNATURE BY COMPARING RECEIVED CARD SIGNATURE FROM EMULATOR WITH EXPECTED SIGNATURE RECEIVED EARLIER FROM SECURITY CARD VIA PAYMENT SERVER
734
CLIENT CODE MODULE GENERATES DEBIT RESULT MESSAGE FOR MERCHANT SERVER
PERFORM STEPS 636 - 640
736
END

FIG. 13

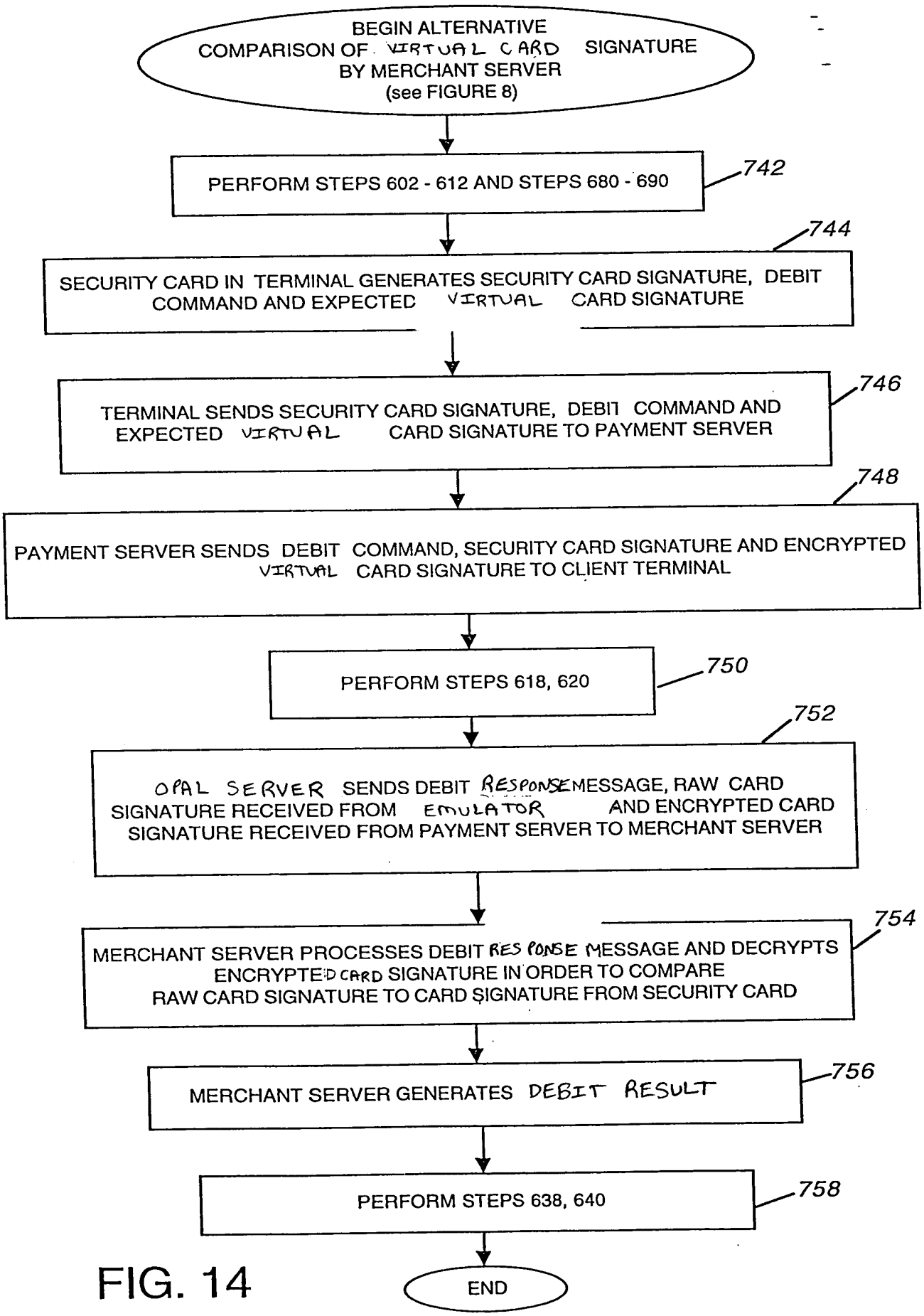

BEGIN ALTERNATIVE COMPARISON OF VIRTUAL CARD SIGNATURE BY MERCHANT SERVER (see FIGURE 8)
PERFORM STEPS 602 - 612 AND STEPS 680 - 690
742
744
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE
TERMINAL SENDS SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE TO PAYMENT SERVER
746
748
PAYMENT SERVER SENDS DEBIT COMMAND, SECURITY CARD SIGNATURE AND ENCRYPTED VIRTUAL CARD SIGNATURE TO CLIENT TERMINAL
PERFORM STEPS 618, 620
750
752
OPAL SERVER SENDS DEBIT RESPONSE MESSAGE, RAW CARD SIGNATURE RECEIVED FROM EMULATOR AND ENCRYPTED CARD SIGNATURE RECEIVED FROM PAYMENT SERVER TO MERCHANT SERVER
754
MERCHANT SERVER PROCESSES DEBIT RESPONSE MESSAGE AND DECRYPTS ENCRYPTED CARD SIGNATURE IN ORDER TO COMPARE RAW CARD SIGNATURE TO CARD SIGNATURE FROM SECURITY CARD
MERCHANT SERVER GENERATES DEBIT RESULT
756
PERFORM STEPS 638, 640
758
END

FIG. 14

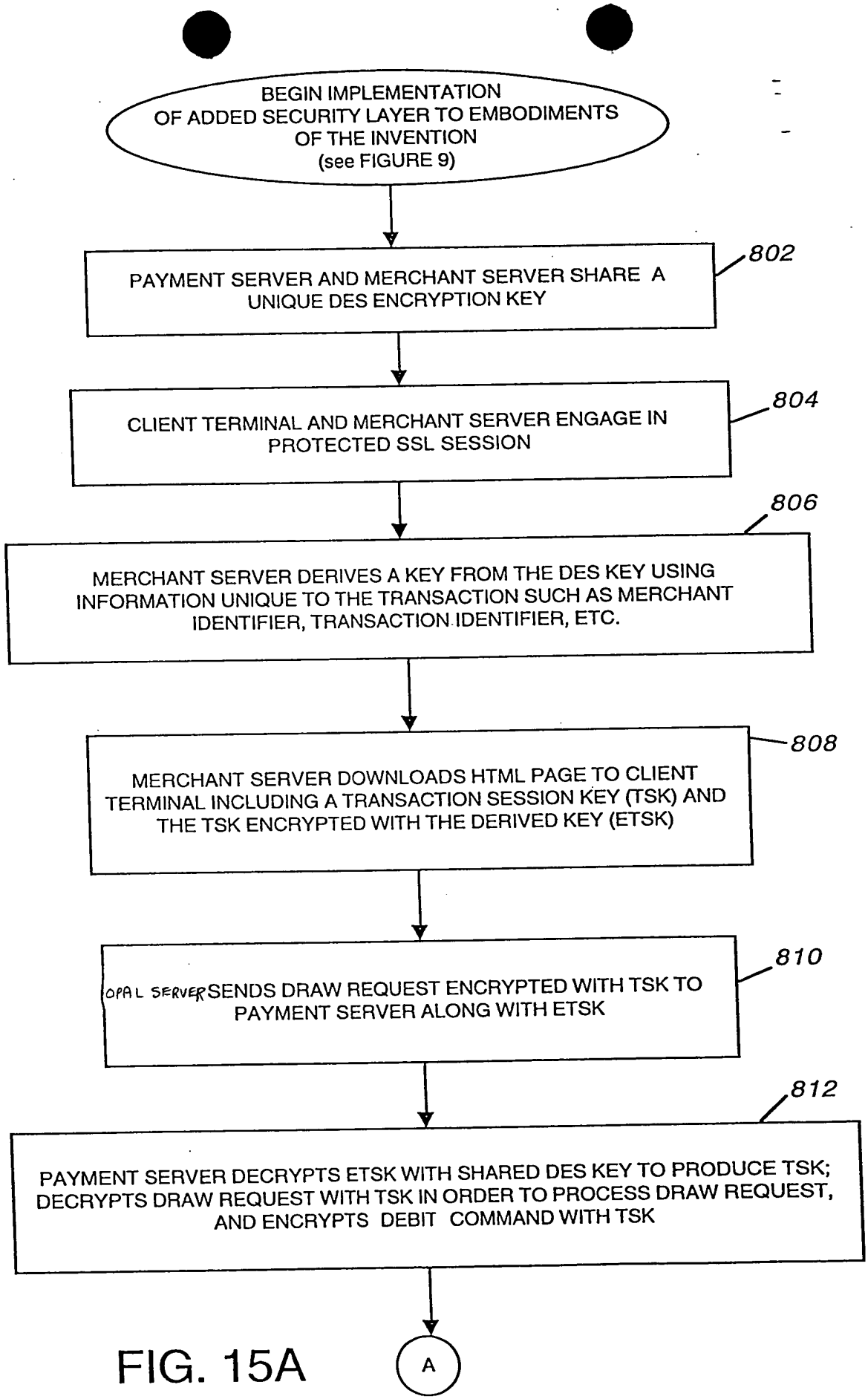

BEGIN IMPLEMENTATION
OF ADDED SECURITY LAYER TO EMBODIMENTS
OF THE INVENTION
(see FIGURE 9)
PAYMENT SERVER AND MERCHANT SERVER SHARE A UNIQUE DES ENCRYPTION KEY
802
CLIENT TERMINAL AND MERCHANT SERVER ENGAGE IN PROTECTED SSL SESSION
804
806
MERCHANT SERVER DERIVES A KEY FROM THE DES KEY USING INFORMATION UNIQUE TO THE TRANSACTION SUCH AS MERCHANT IDENTIFIER, TRANSACTION IDENTIFIER, ETC.
MERCHANT SERVER DOWNLOADS HTML PAGE TO CLIENT TERMINAL INCLUDING A TRANSACTION SESSION KEY (TSK) AND THE TSK ENCRYPTED WITH THE DERIVED KEY (ETSK)
808
OPAL SERVER SENDS DRAW REQUEST ENCRYPTED WITH TSK TO PAYMENT SERVER ALONG WITH ETSK
810
812
PAYMENT SERVER DECRYPTS ETSK WITH SHARED DES KEY TO PRODUCE TSK; DECRYPTS DRAW REQUEST WITH TSK IN ORDER TO PROCESS DRAW REQUEST, AND ENCRYPTS DEBIT COMMAND WITH TSK
A

FIG. 15A

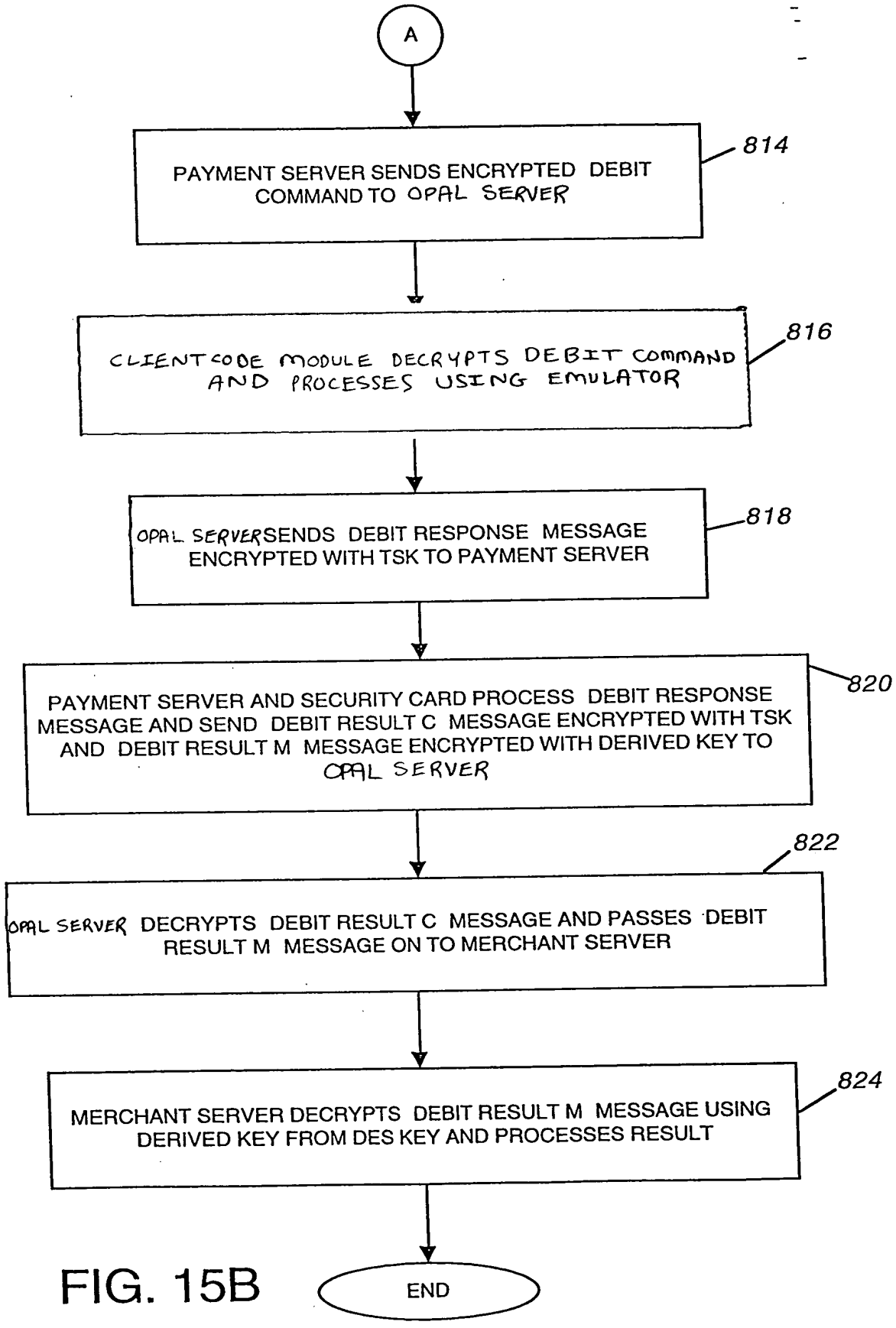

A
PAYMENT SERVER SENDS ENCRYPTED DEBIT COMMAND TO OPAL SERVER
814
CLIENT CODE MODULE DECRYPTS DEBIT COMMAND AND PROCESSES USING EMULATOR
816
OPAL SERVER SENDS DEBIT RESPONSE MESSAGE ENCRYPTED WITH TSK TO PAYMENT SERVER
818
PAYMENT SERVER AND SECURITY CARD PROCESS DEBIT RESPONSE MESSAGE AND SEND DEBIT RESULT C MESSAGE ENCRYPTED WITH TSK AND DEBIT RESULT M MESSAGE ENCRYPTED WITH DERIVED KEY TO OPAL SERVER
820
822
OPAL SERVER DECRYPTS DEBIT RESULT C MESSAGE AND PASSES DEBIT RESULT M MESSAGE ON TO MERCHANT SERVER
MERCHANT SERVER DECRYPTS DEBIT RESULT M MESSAGE USING DERIVED KEY FROM DES KEY AND PROCESSES RESULT
824
END

FIG. 15B

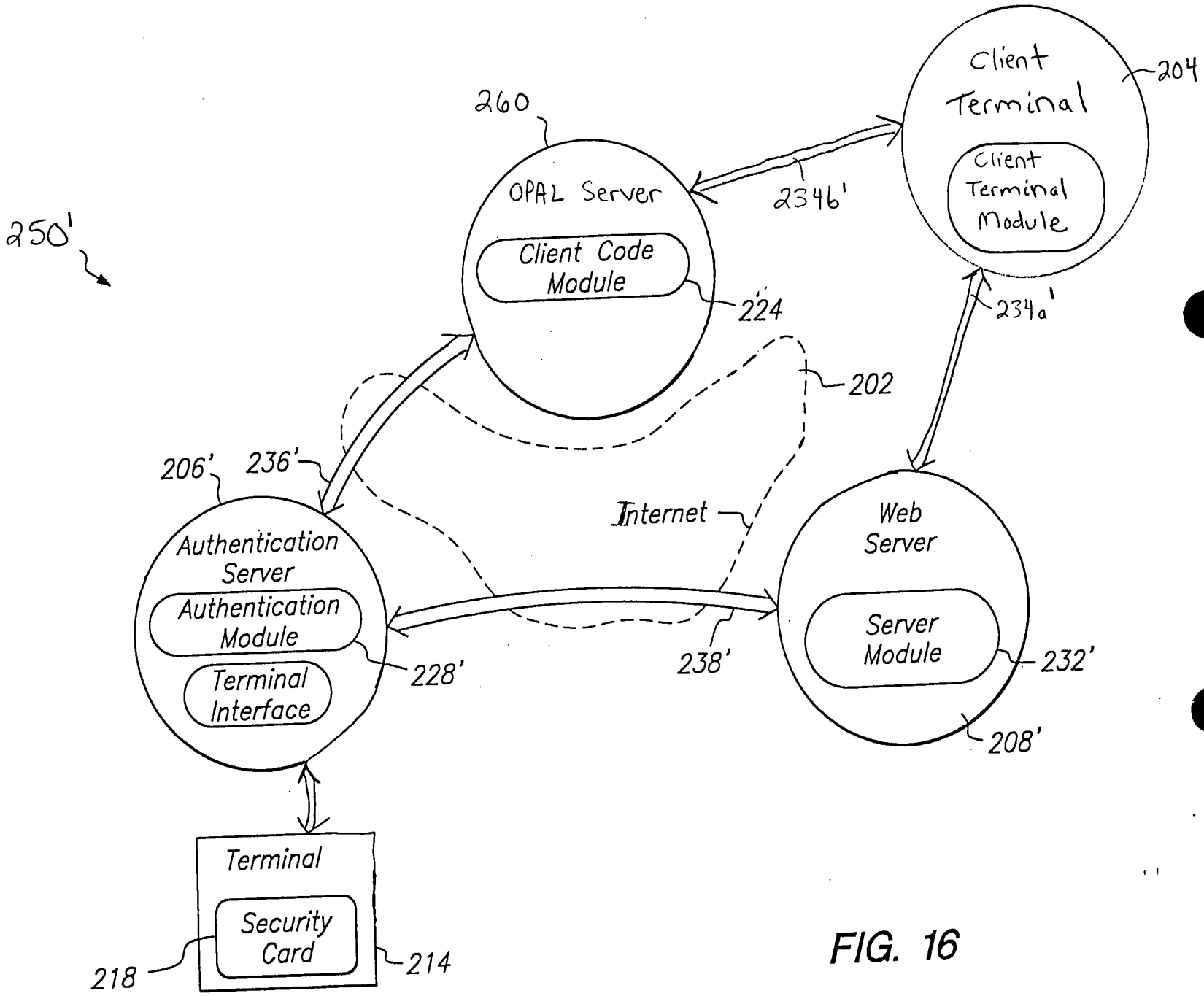

250'
260
OPAL Server
Client Code Module
224
Client Terminal
204
Client Terminal Module
234a'
234b'
202
206'
236'
Internet
Authentication Server
Authentication Module
Terminal Interface
228'
238'
Web Server
Server Module
232'
208'
Terminal
Security Card
218
214

FIG. 16

FIG. 17

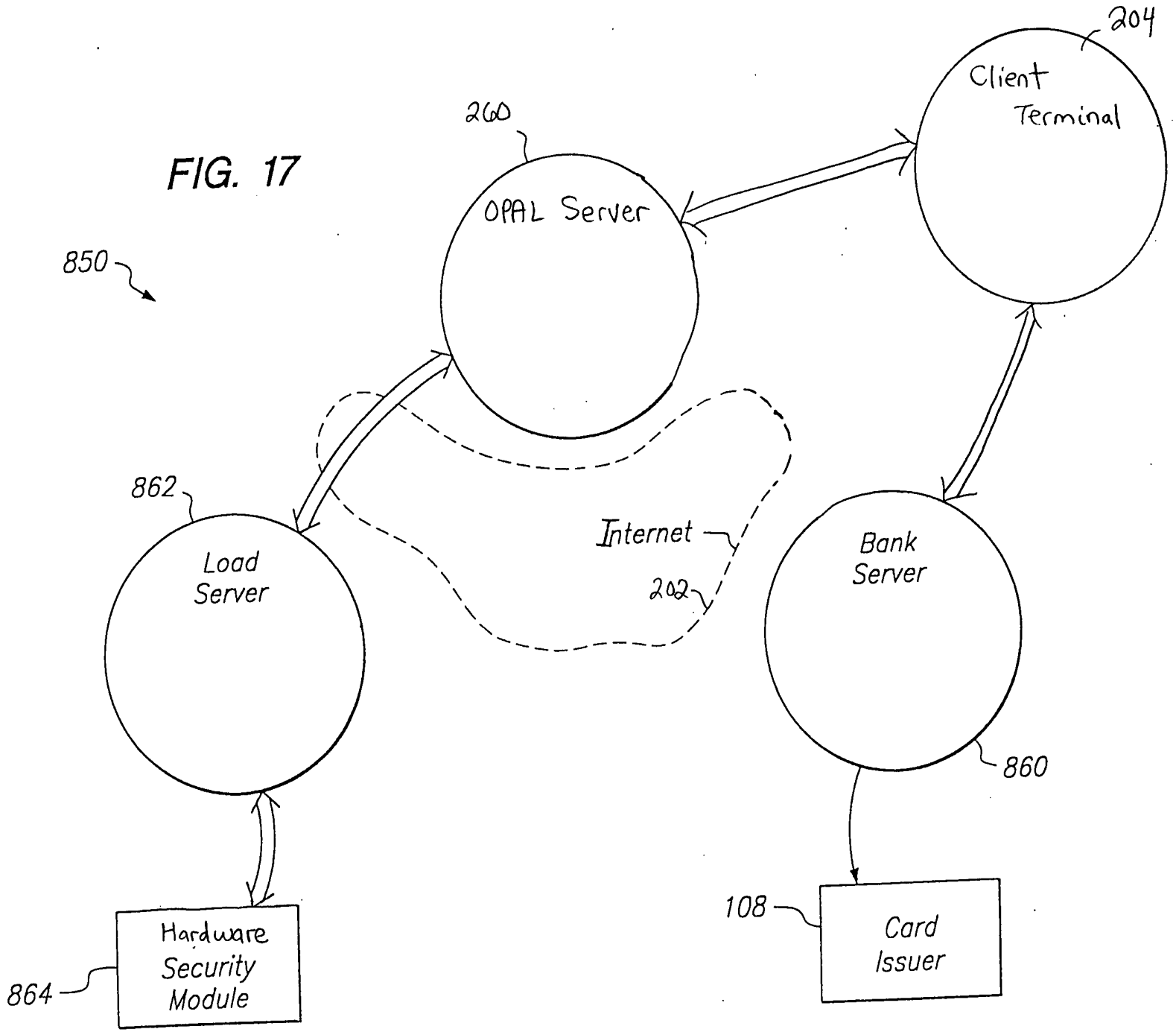


FIG. 18A

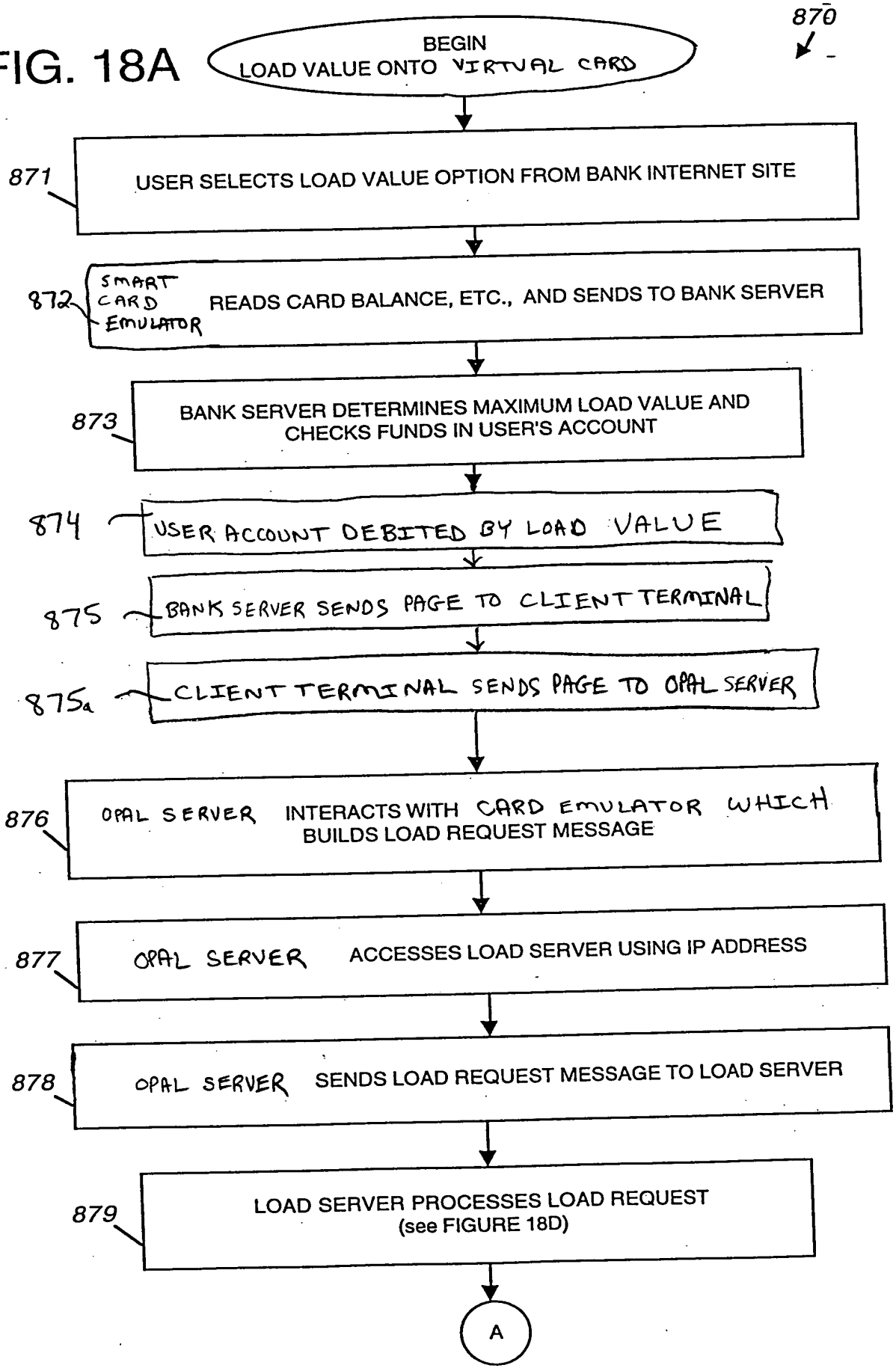

870
BEGIN
LOAD VALUE ONTO VIRTUAL CARD
871
USER SELECTS LOAD VALUE OPTION FROM BANK INTERNET SITE
872
SMART CARD EMULATOR
READS CARD BALANCE, ETC., AND SENDS TO BANK SERVER
873
BANK SERVER DETERMINES MAXIMUM LOAD VALUE AND CHECKS FUNDS IN USER'S ACCOUNT
874
USER ACCOUNT DEBITED BY LOAD VALUE
875
BANK SERVER SENDS PAGE TO CLIENT TERMINAL
875a
CLIENT TERMINAL SENDS PAGE TO OPAL SERVER
876
OPAL SERVER INTERACTS WITH CARD EMULATOR WHICH BUILDS LOAD REQUEST MESSAGE
877
OPAL SERVER ACCESSES LOAD SERVER USING IP ADDRESS
878
OPAL SERVER SENDS LOAD REQUEST MESSAGE TO LOAD SERVER
879
LOAD SERVER PROCESSES LOAD REQUEST
(see FIGURE 18D)
A

FIG. 18B

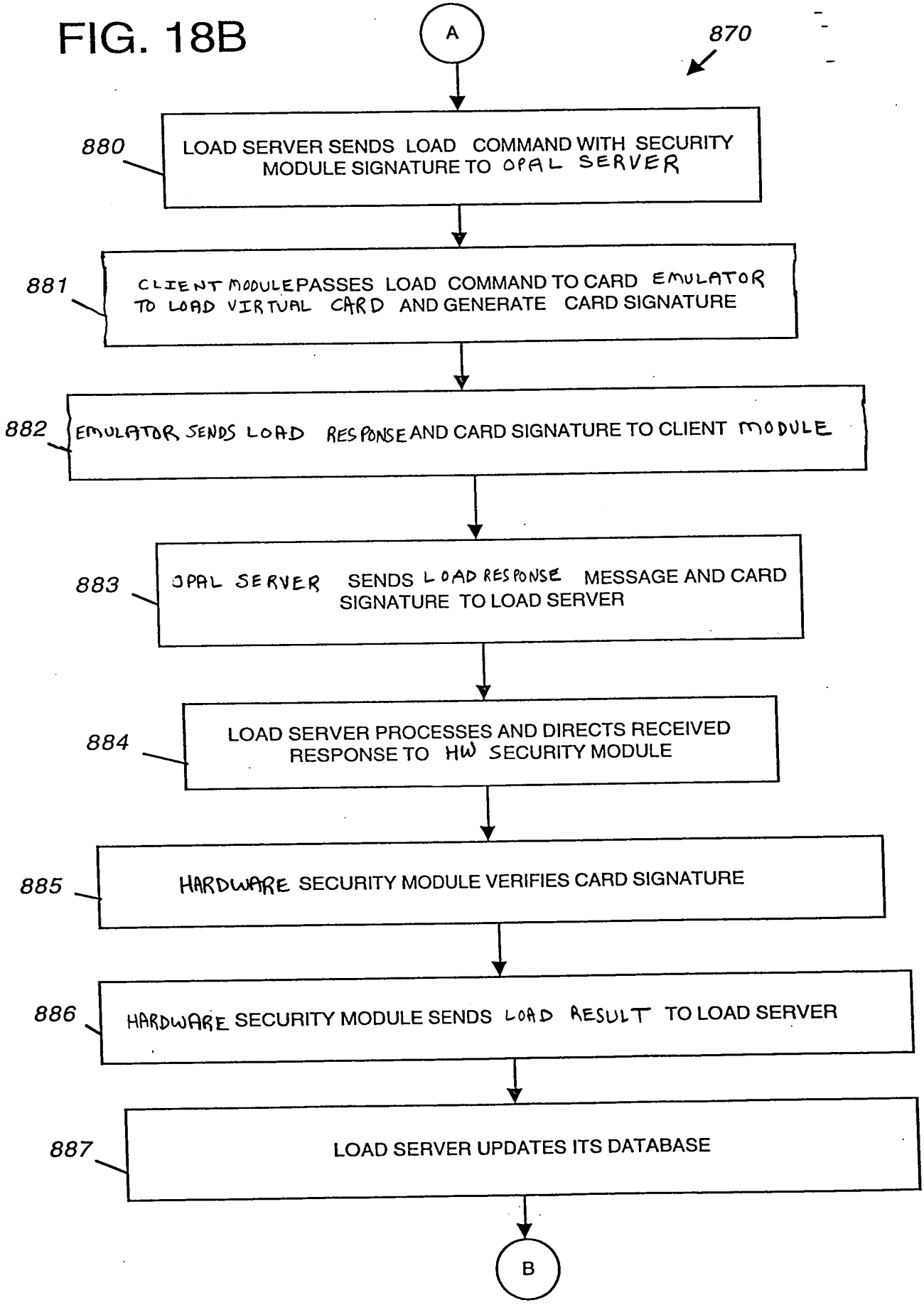
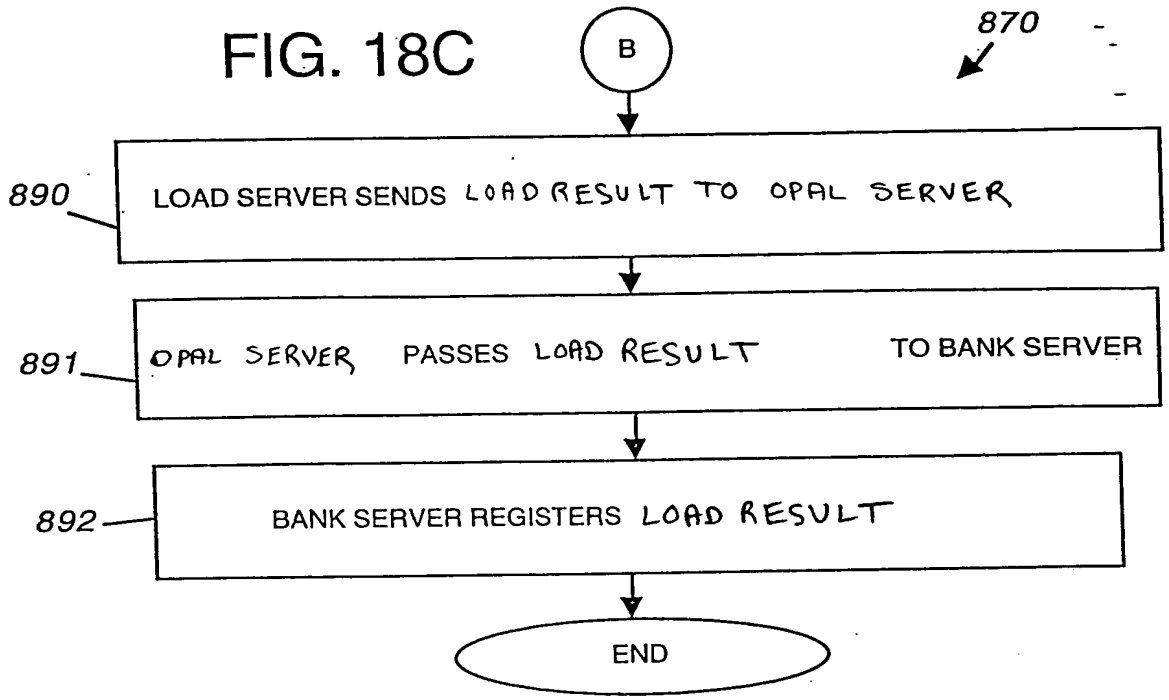


FIG. 18C



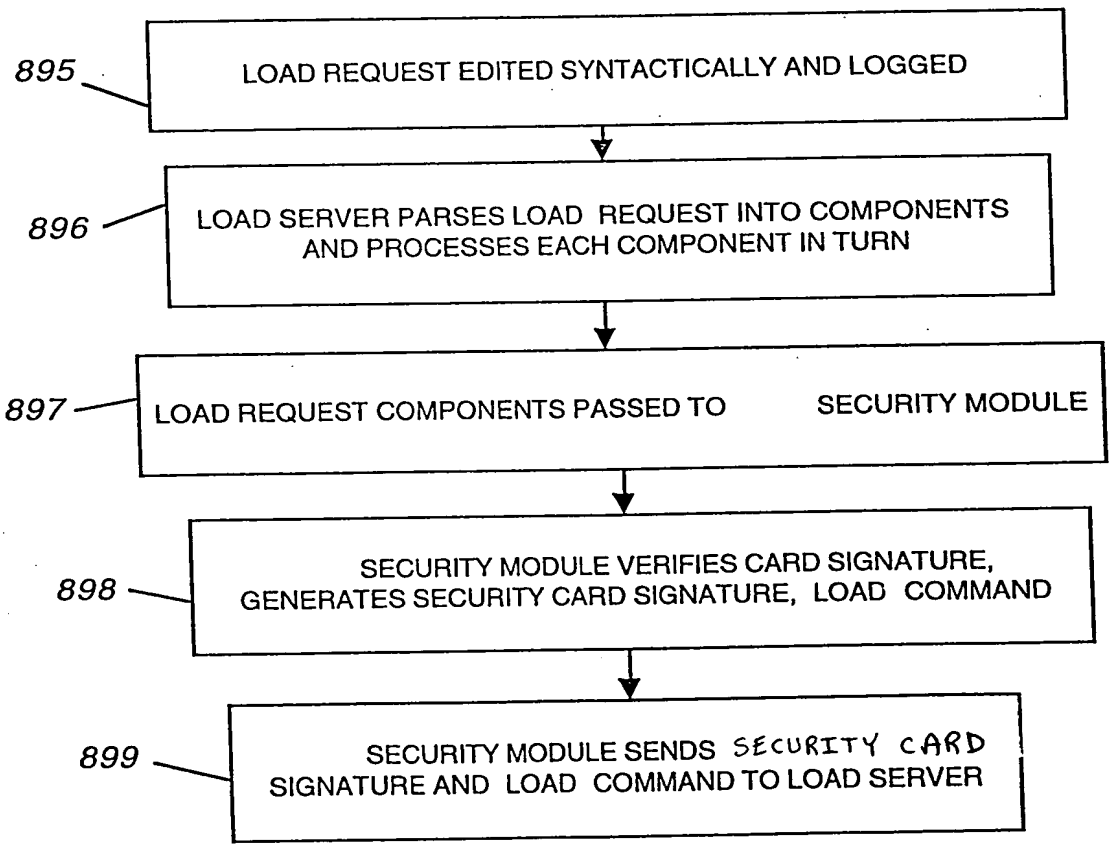


FIG. 18D

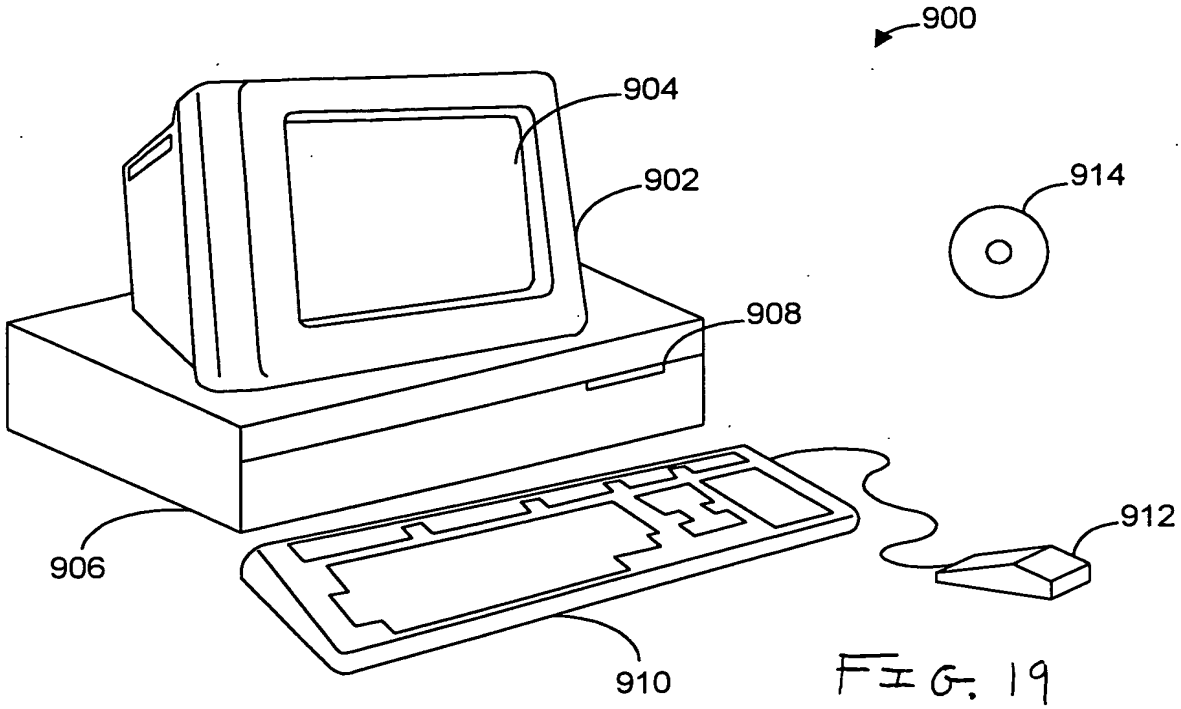

900
904
902
914
908
912
906
910

FIG. 19

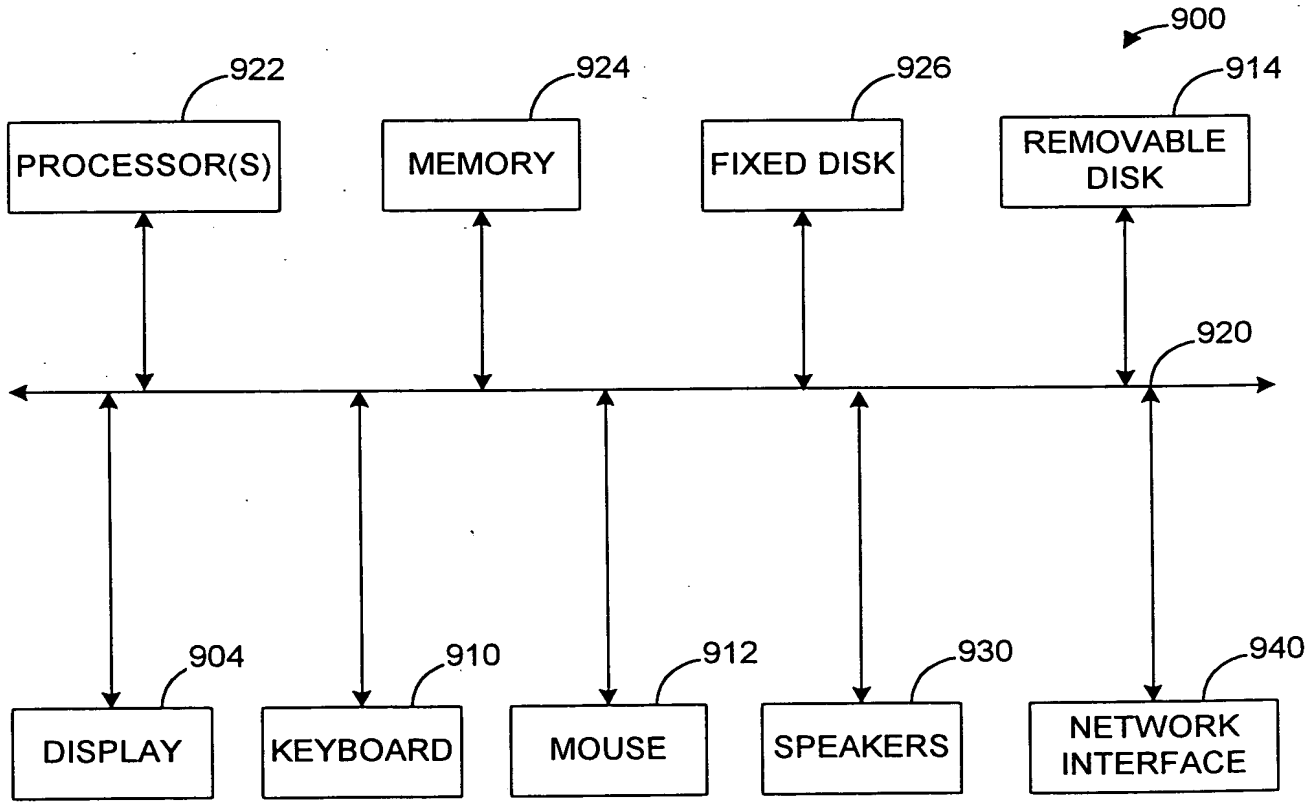

900
922
924
926
914
PROCESSOR(S)
MEMORY
FIXED DISK
REMOVABLE DISK
920
904
910
912
930
940
DISPLAY
KEYBOARD
MOUSE
SPEAKERS
NETWORK INTERFACE

FIG. 20